2017

Galois module structure for Artin-Schreier theory over bicyclic extensions

Lauren Heller
lheller@wellesley.edu

Galois module structure for Artin-Schreier theory over bicyclic extensions

Lauren Cranton Heller
advisor: Professor Andrew Schultz

submitted in partial fulfillment of the prerequisite for honors

Department of Mathematics
Wellesley College
April 2017

Abstract

If K/F is a Galois field extension with Galois group of order p^n where $p \neq \text{char}(F)$, then $\text{Gal}(K/F)$ acts on the quotient $K^\times/K^{\times p}$. The structure of this $\mathbb{F}_p[\text{Gal}(K/F)]$-module is known for $\text{Gal}(K/F)$ isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$ or the Klein 4-group. We use Artin-Schreier theory to produce a similar decomposition for characteristic p extensions with $\text{Gal}(K/F)$ isomorphic to $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$.

Acknowledgements

Andrew Schultz for sharing his work and his time with me; Alexander Diesl and Karen Lange for serving on my committee; Bridget Schreiner for her mathematical and non-mathematical camaraderie; Simona Boyadzhiyska for encouraging me to write a thesis; Donald Elmore for his excellent advice; and Lisa, Thomas, and Megan Heller for their constant support

Contents

Chapter 1

Introduction

Galois theory assigns to each field extension an automorphism group, and this process is well understood. Thus one might ask the inverse question: given a group, what sorts of field extensions give rise to it? We will tackle a small part of this problem by specifying the structure of a module that can be constructed from an extension and its Galois group.

In particular, we are interested in bicyclic extensions, those with Galois group of the form $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$ for a prime p, where the characteristic of the ground field matches the exponent p of the group. Such extensions are described by Artin-Schreier theory, which we will cover briefly in this chapter. It is a variant of the more common Kummer theory, which covers extensions with Galois group $\bigoplus_i \mathbb{Z}/p^{n_i}\mathbb{Z}$ where the characteristic is not p.

The decomposition of the analagous Kummer-theoretic module is known when the Galois group is $\mathbb{Z}/p^n\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ (the Klein 4-group), and the latter proof by Chemotti ([1]) inspired much of this work. Since Kummer theory is more classical than Artin-Schreier theory, we will begin there.

1.1 Kummer theory

If F is a field containing p distinct p-th roots of unity for some prime $p \neq \mathrm{char}(F)$ and $\sqrt[p]{a}$ is the formal root of an irreducible polynomial $x^p - a \in F[x]$, then the Galois group of the field extension $F(\sqrt[p]{a})/F$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. Kummer theory says that the converse is also true: if K/F is a Galois field extension with $\mathrm{Gal}(K/F) \cong \mathbb{Z}/p\mathbb{Z}$ for some $p \neq \mathrm{char}(F)$ and F contains the p-th roots of unity, then there exists $a \in F$ such that $K \cong F(\sqrt[p]{a})$ where $\sqrt[p]{a}$ is a root of $x^p - a$.

Let $F^{\times p} = \{f^p : f \in F^\times\}$, ie. the units in F with p-th roots also in F. This is a normal subgroup of the multiplicative group of units $F^\times$, and there is a bijection between finite subgroups of $F^\times/F^{\times p}$ and extensions over F with finite Abelian Galois group of exponent dividing p. Given a subgroup $U \leq F^\times/F^{\times p}$ we can obtain such an extension by adjoining to F the roots of all polynomials of the form $x^p - a$ for $aF^{\times p} \in U$.

Conversely, given an extension K/F with $\mathrm{Gal}(K/F)$ finite, Abelian, and of exponent dividing p, we can obtain a subgroup of $F^\times/F^{\times p}$ by taking all elements $aF^{\times p}$ such that $a \in F \cap K^{\times p}$. Kummer theory says that these processes are inverses of each other. In particular, the extension $F(\sqrt[p]{a})/F$ is associated with the subgroup generated by $aF^{\times p}$ in

$F^\times/aF^{\times p}$, namely the cosets with representatives $1, a, a^2, \ldots, a^{p-1}$.

The Galois group of an extension K/F acts on elements of $K^\times$, so $K^\times$ is a module over the group ring $\mathbb{Z}[\mathrm{Gal}(K/F)]$, which consists of formal $\mathbb{Z}$ linear combinations of elements in $\mathrm{Gal}(K/F)$ and acts by the following:

$$k^{\sum \alpha_i\sigma_i} = \prod \sigma_i^{\alpha_i}(k)$$

If $\sum \alpha_i\sigma_i$ is in the ideal $p\mathbb{Z}[\mathrm{Gal}(K/F)]$, then $[k]^{\sum \alpha_i\sigma_i} = [0]$ in $K^\times/K^{\times p}$ for all $k \in K$, so this action descends to an action on $K^\times/K^{\times p}$ by

$$\frac{\mathbb{Z}[\mathrm{Gal}(K/F)]}{p\mathbb{Z}[\mathrm{Gal}(K/F)]} \cong \mathbb{F}_p[\mathrm{Gal}(K/F)].$$

As stated above, the structure of $K^\times/K^{\times p}$ as an $\mathbb{F}_p[\mathrm{Gal}(K/F)]$-module is known when $\mathrm{Gal}(K/F) \cong \mathbb{Z}/p^n\mathbb{Z}$ for $\mathrm{char}(F) \neq p$ (Theorems 1 and 2 in [3]) and when $\mathrm{Gal}(K/F) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ for $\mathrm{char}(F) \neq 2$ ([1]).

1.2 Artin-Schreier theory

If F is a field of characteristic p, then polynomials of the form $x^p - a \in F[x]$ are not separable. (Given a single root θ_a they can be factored as $(x-\theta_a)^p$.) Instead, Galois groups isomorphic to $\mathbb{Z}/p\mathbb{Z}$ arise as extensions $F(\theta_a)/F$ where θ_a is a root of an irreducible and separable polynomial $x^p - x - a \in F[x]$.

Theorem 1.1. *If θ_a is a root of the polynomial $x^p - x - a \in F[x]$ and $\mathrm{char}\, F = p$, then $\theta_a + 1$ is another root.*

Proof. Suppose θ_a is a root of $x^p - x - a$. Then

$$(\theta_a + 1)^p - (\theta_a + 1) - f = \theta_a^p + 1^p - \theta_a - 1 - a = \theta_a^p - \theta_a - a = 0$$

because $F(\theta_a)$ has characteristic p. □

Thus the roots of $x^p - x - a$ are $\theta_a, \theta_a + 1, \ldots, \theta_a + p - 1$, so $F(\theta_a)$ is a splitting field and we no longer need to require that F contain p-th roots of unity. The relevant normal subgroup is contained in K^+, the group of K under addition.

Definition 1. If K is a field, let $\wp(K) = \{k^p - k : k \in K\}$.

We can now state the central result of the theory.

Theorem 1.2 (Artin-Schreier)**.** *A Galois field extension K/F of characteristic p has cyclic Galois group of order p if and only if it is the splitting field of an irreducible polynomial $x^p - x - a$ for some $a \in F$. Furthermore, there is a bijection between finite subgroups of the quotient $F^+/\wp(F)$ and finite Abelian extensions over F with exponent dividing p.*

The bijective correspondence is given by

$$U \mapsto F(\theta_a : a + \wp(F) \in U)$$

where θ_a is a root of the polynomial $x^p - x - a$, and inversely,

$$K/F \mapsto \{a + \wp(F) : a \in F \cap \wp(K)\}.$$

In particular, the extension $F(\theta_a)/F$ is associated with the subgroup generated by $a + \wp(F)$ in $F^+/\wp(F)$, namely

$$\{\wp(F), a + \wp(F), 2a + \wp(F), \ldots, (p-1)a + \wp(F)\}.$$

Moving from traditional Artin-Schreier theory to the subject of our research, the group ring $\mathbb{F}_p[\mathrm{Gal}(K/F)]$ corresponding to an extension K/F with Galois group of order p^n for $p = \mathrm{char}(F)$ acts on the quotient $K^+/\wp(K)$, this time additively:

$$\left(\sum \alpha_i \sigma_i\right)[k] = \left[\sum \alpha_i \sigma_i(k)\right]$$

The structure of $K^+/\wp(K)$ as an $\mathbb{F}_p[\mathrm{Gal}(K/F)]$-module is known when $\mathrm{Gal}(K/F) \cong \mathbb{Z}/p^n\mathbb{Z}$ (Prop. 6.2 in [2]).

1.3 Main theorem

The primary result of this thesis is to provide the first module decomposition for $K^+/\wp K$ when $\mathrm{Gal}(K/F)$ is a noncyclic p-group.

Theorem 1.3. *Let K/F be a Galois field extension of characteristic p with $\mathrm{Gal}(K/F) \cong \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$. Then $K^+/\wp(K) \cong X \oplus Y$ as an $\mathbb{F}_p[\mathrm{Gal}(K/F)]$-module for Y a direct sum of free modules and X an indecomposable module with $\mathbb{F}_p$-dimension $p^2 + 1$ and presentation $\langle x_L, x_R : (\sigma - 1)x_L = (\tau - 1)x_R \rangle$.*

After some background information in Chapter 2, this will be restated and proven for $p = 2$ in Chapter 3 and for odd p in Chapter 4.

Chapter 2

Preliminaries

2.1 Trace maps

Since the only ideals of a field are $\{0\}$ and the field itself, the only nontrivial ring homomorphisms between subfields of an extension K/F are isomorphisms, which can be extended to automorphisms in $\mathrm{Gal}(K/F)$, and inclusion maps. To find a map from K to a proper subfield we must relax the requirement that it preserve both additive and multiplicative structure. One such map is constructed from the elements of $\mathrm{Gal}(K/F)$.

Definition 2. Let K/F be a Galois extension with Galois group G and let $k \in K$. Then

$$T_{K/F}(k) = \sum_{\sigma \in G} \sigma(k)$$

is known as the *trace* from K to F.

Note that the trace map $T_{K/F}$ from K to F is a homomorphism on the additive group K^+.

Theorem 2.1. *Let K/F be a Galois extension and let $k \in K$. Then $T_{K/F}(k) \in F$.*

Proof. Let $G = \mathrm{Gal}(K/F)$ and suppose $\tau \in G$. Then applying τ to the elements of G simply permutes them, so

$$\tau(T_{K/F}(k)) = \tau\left(\sum_{\sigma \in G} \sigma(k)\right) = \sum_{\sigma \in G} (\tau \circ \sigma)(k) = \sum_{\sigma \in G} \sigma(k) = T_{K/F}(k).$$

Thus $T_{K/F}(k)$ is fixed by all elements of $\mathrm{Gal}(K/F)$, which implies that $T_{K/F}(k) \in F$ because K/F is Galois. □

Though we will not prove it in full generality, if $K/M/F$ is a tower of Galois field extensions, then $T_{M/F} \circ T_{K/M} = T_{K/F}$. The map $T_{K/F}$ also respects equivalence classes as follows:

Corollary 2.2. *If $k_1 + \wp(K) = k_2 + \wp(K)$ then $T_{K/F}(k_1) + \wp(F) = T_{K/F}(k_2) + \wp(F)$.*

Proof. If $k_1 + \wp(K) = k_2 + \wp(K)$ then there exists $k \in K$ such that $k_1 - k_2 = k^p - k$. Thus

$$T_{K/F}(k_1) - T_{K/F}(k_2) = T_{K/F}(k_1 - k_2) = T_{K/F}(k^p - k) = (T_{K/F}(k))^p - T_{K/F}(k) \in \wp(F)$$

because $T_{K/F}$ is a homomorphism and $T_{K/F}(k) \in F$, so $T_{K/F}(k_1) + \wp(F) = T_{K/F}(k_2) + \wp(F)$. (Note that $T_{K/F}(k^p) = (T_{K/F}(k))^p$ because $\operatorname{char} K = p$.) □

We will use this fact to classify elements of our module according to their images in subfields of K. For the particular field extensions of interest to us, trace maps are in fact surjective on elements, which we will first prove for cyclic extensions.

Theorem 2.3. *Let K/F be a Galois field extension of characteristic p with $\mathrm{Gal}(K/F) \simeq \mathbb{Z}/p\mathbb{Z}$. Then $T_{K/F}\colon K \to F$ is surjective.*

Proof. Let σ be a generator of $\mathbb{Z}/p\mathbb{Z}$ and let $\theta \in K$ such that $K = F(\theta)$. We will show that

$$T_{K/F}(\theta^i) = \begin{cases} 0 & i \neq p-1 \\ -1 & i = p-1. \end{cases}$$

Choose σ so that $\sigma(\theta) = \theta + 1$. By the binomial theorem

$$\begin{aligned} T_{K/F}(\theta^i) &= (1 + \sigma + \sigma^2 + \cdots + \sigma^{p-1})(\theta^i) \\ &= \theta^i + (\theta+1)^i + (\theta+2)^i + \cdots + (\theta+p-1)^i \\ &= \theta^i + \sum_{j=0}^{i} \binom{i}{j}\theta^{i-j} + \sum_{j=0}^{i} \binom{i}{j}\theta^{i-j}2^j + \cdots + \sum_{j=0}^{i} \binom{i}{j}\theta^{i-j}(p-1)^j \\ &= p\theta^i + \theta^{i-1}\sum_{\ell=1}^{p-1}\binom{i}{1}\ell + \theta^{i-2}\sum_{\ell=1}^{p-1}\binom{i}{2}\ell^2 + \cdots + \theta\sum_{\ell=1}^{p-1}\binom{i}{j-1}\ell^{j-1} + \sum_{\ell=1}^{p-1}\binom{i}{j}\ell^j \end{aligned}$$

The image of the map $\mathbb{F}_p^\times \to \mathbb{F}_p^\times$ given by $\ell \mapsto \ell^j$ is cyclic. Let g be a generator. Then

$$\sum_{\ell=1}^{p-1}\binom{i}{j}\ell^j = \binom{i}{j}\sum_{k=1}^{p-1} g^k = g\binom{i}{j}\sum_{k=1}^{p-1} g^k$$

because the order of g divides $p-1$, so

$$0 = (g-1)\binom{i}{j}\sum_{k=1}^{p-1} g^k = (g-1)\sum_{\ell=1}^{p-1}\binom{i}{j}\ell^j.$$

We have $g = 1$ if and only if $j = p-1$, so the coefficient of θ^{i-j} in $T_{K/F}(\theta^i)$ is 0 modulo p for $j \neq p-1$. For $j = p-1$

$$\sum_{\ell=1}^{p-1}\binom{i}{j}\ell^j = \binom{i}{p-1}\sum_{\ell=1}^{p-1}\ell^{p-1} = \binom{i}{p-1}\sum_{\ell=1}^{p-1} 1 = (p-1)\binom{i}{p-1}$$

by Fermat's Little Theorem. This is equal to 0 for $i \neq p-1$ (ie. $(p-1)$-th powers do not appear in the original sum). If $i = p-1$ then it is equal to $p-1 \equiv -1 \mod p$. Thus

$T_{K/F}(\theta^i) = 0$ for $i \neq p-1$ and the only nonzero term of $T_{K/F}(\theta^{p-1})$ is the constant -1.

Suppose $f \in F$. Then $-f\theta^{p-1} \in K$ and

$$T_{K/F}(-f\theta^{p-1}) = -fT_{K/F}(\theta^{p-1}) = -f(-1) = f$$

so $T_{K/F}$ is surjective. □

Corollary 2.4. *Let K/F be a Galois field extension of characteristic p with*

$$\mathrm{Gal}(K/F) \simeq \mathbb{Z}/p^{n_1}\mathbb{Z} \oplus \mathbb{Z}/p^{n_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{n_k}\mathbb{Z}$$

for some positive integers $n_1, \ldots, n_k$. Then $T_{K/F}$ is surjective.

Proof. Let $m = n_1 + \cdots + n_k$ (the power of p in the degree of K/F) and consider the tower $K = L_0 \supset L_1 \supset \cdots \supset L_m = F$ of intermediate fields corresponding to the subgroups

$$\begin{gathered}
\mathbb{Z}/p^{n_1}\mathbb{Z} \oplus \mathbb{Z}/p^{n_2} \oplus \cdots \oplus \mathbb{Z}/p^{n_k}\mathbb{Z} \\
p\mathbb{Z}/p^{n_1}\mathbb{Z} \oplus \mathbb{Z}/p^{n_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{n_k}\mathbb{Z} \\
\vdots \\
p^{n_1-1}\mathbb{Z}/p^{n_1}\mathbb{Z} \oplus \mathbb{Z}/p^{n_2}\mathbb{Z} \cdots \oplus \mathbb{Z}/p^{n_k}\mathbb{Z} \\
0 \oplus \mathbb{Z}/p^{n_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{n_k}\mathbb{Z} \\
0 \oplus p\mathbb{Z}/p^{n_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{n_k}\mathbb{Z} \\
\vdots \\
0 \oplus 0 \oplus \cdots \oplus \mathbb{Z}/p^{n_k}\mathbb{Z} \\
\vdots \\
0 \oplus 0 \oplus \cdots \oplus 0
\end{gathered}$$

of $\mathrm{Gal}(K/F)$, so that $\mathrm{Gal}(L_i/L_{i+1}) \simeq \mathbb{Z}/p\mathbb{Z}$ for all i. Then $T_{L_i/L_{i+1}}$ is surjective for all i by the theorem above, and

$$T_{K/F} = T_{L_0/L_m} = T_{L_{m-1}/L_m} \circ \cdots \circ T_{L_1/L_2} \circ T_{L_0/L_1}$$

so $T_{K/F}$ is also surjective. □

2.2 Properties of modules

For the purposes of this section, let $G = \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z} = \langle \sigma, \tau \rangle$ for some prime p, let M, N be modules over the group ring $\mathbb{F}_p[G]$, and denote by M^G the submodule of M fixed under action by G. We will prove general results about these modules to be used later.

Lemma 2.5. *We have $M^G \cap N^G = \{0\}$ if and only if $M \cap N = \{0\}$.*

Proof. Clearly $M \cap N = \{0\}$ implies $M^G \cap N^G = \{0\}$. We will prove the converse by contrapositive. Let $y \in M \cap N$ be nonzero.

Since G is finite, there exists a smallest positive integer i such that $(\sigma-1)^i y = 0$. Consider $(\sigma-1)^{i-1}y$. By choice of i, this element is nonzero and fixed by σ. Similarly, let j be the smallest positive integer such that $(\tau-1)^j(\sigma-1)^{i-1}y = 0$. Then $(\tau-1)^{j-1}(\sigma-1)^{i-1}y$ is nonzero and fixed by σ and τ.

Since M and N are closed under action by G, we have $(\tau-1)^{j-1}(\sigma-1)^{i-1}y \in M^G \cap N^G$. Therefore $M^G \cap N^G \neq \{0\}$. □

Lemma 2.6. *Suppose M and N are submodules of a single $\mathbb{F}_p[G]$-module and $M \cap N = \{0\}$. Then $(M \oplus N)^G = M^G \oplus N^G$.*

Proof. Suppose $x \in M^G \oplus N^G$. Then there exist $m \in M^G$ and $n \in N^G$ such that $x = m+n$, so

$$\sigma(x) = \sigma(m+n) = \sigma(m) + \sigma(n) = m + n = x$$

and similarly $\tau(x) = x$. Thus $M^G \oplus N^G \subseteq (M \oplus N)^G$.

Now suppose $x \in (M \oplus N)^G$. Then $x \in M \oplus N$, so there exist $m \in M$ and $n \in N$ such that $x = m + n$, so

$$m + n = x = \sigma(x) = \sigma(m+n) = \sigma(m) + \sigma(n)$$

where $\sigma(m) \in M$ and $\sigma(n) \in N$. Since the representation $m+n$ is unique, we must have $\sigma(m) = m$ and $\sigma(n) = n$. Similarly $\tau(m) = m$ and $\tau(n) = n$, so $(M \oplus N)^G \subseteq M^G \oplus N^G$. □

Lemma 2.7. *Each element of $\mathbb{F}_p[G]$ can be written in the form*

$$\sum_{i=0}^{p-1}\sum_{j=0}^{p-1} \alpha_{ij}(\sigma-1)^i(\tau-1)^j$$

for some $\alpha_{ij} \in \mathbb{F}_p$.

Proof. We will first show that each element $\sum_{i=1}^{p-1}\beta_i\sigma^i$ of $\mathbb{F}_p[\langle\sigma\rangle]$ can be written in the form $\sum_{i=1}^{p-1}\alpha_i(\sigma-1)^i$ for some $\alpha_i \in \mathbb{F}_p$. This amounts to a change in $\mathbb{F}_p$-basis.

Note that $(\sigma-1)^i$ has degree i as a polynomial in σ. Thus the matrix representing the transition from $\{1, (\sigma-1), (\sigma-1)^2, \ldots, (\sigma-1)^{p-1}\}$ to $\{1, \sigma, \sigma^2, \ldots, \sigma^{p-1}\}$ is triangular and has no nonzero entries on the diagonal, so it is invertible.

Since each term of an element $\sum_{i=1}^{p-1}\sum_{j=1}^{p-1}\beta_{ij}\sigma^i\tau^j$ in $\mathbb{F}_p[\mathrm{Gal}(K/F)]$ can be written as the product of an element in $\mathbb{F}_p[\langle\sigma\rangle]$ and one in $\mathbb{F}_p[\langle\tau\rangle]$, and products of elements of the form $\sum_{i=0}^{p-1}\sum_{j=0}^{p-1}\alpha_{ij}(\sigma-1)^i(\tau-1)^j$ also have this form, the lemma follows. □

This representation of elements in $\mathbb{F}_p[G]$ is convenient because an element in an $\mathbb{F}_p[G]$-module is fixed if and only if it is killed by $\sigma-1$ and $\tau-1$. We will also frequently use the fact that $(\sigma-1)^p = \sigma^p - 1 = 0$ and $(\tau-1)^p = \tau^p - 1 = 0$ in characteristic p.

The remainder of the results in this section will be technical and very poorly motivated because they concern a specific module X that we have not yet constructed. Proofs about the properties of this X are somewhat neater in a general setting and will be referenced, as one might guess, in Sections 3.4 and 4.4, both labeled "Construction of X."

Lemma 2.8. *Let X be an $\mathbb{F}_p[G]$-module with generators α_L and α_R satisfying $(\sigma-1)\alpha_L = (\tau-1)\alpha_R$ such that the elements $(\tau-1)^{p-1}\alpha_L$, $(\sigma-1)^{p-1}\alpha_R$, and $(\sigma-1)^{p-1}(\tau-1)^{p-2}\alpha_L$ are nonzero.*

Then a nonzero element of the form $(\sigma-1)^i(\tau-1)^j\alpha_L$ is in X^G if and only if either $i=0$ and $j=p-1$ or $i=p-1$ and $j=p-2$. Similarly a nonzero element $(\sigma-1)^i(\tau-1)^j\alpha_R$ is in X^G if and only if either $i=p-1$ and $j=0$ or $i=p-2$ and $j=p-1$.

Proof. We have

$$\begin{aligned}(\sigma-1)(\tau-1)^{p-1}\alpha_L &= (\tau-1)^p\alpha_R\\ (\tau-1)(\tau-1)^{p-1}\alpha_L &= (\tau-1)^p\alpha_L\\ (\sigma-1)(\sigma-1)^{p-1}(\tau-1)^{p-2}\alpha_L &= (\sigma-1)^p(\tau-1)^{p-2}\alpha_L\\ (\tau-1)(\sigma-1)^{p-1}(\tau-1)^{p-2}\alpha_L &= (\sigma-1)^{p-2}(\tau-1)^p\alpha_R\end{aligned}$$

where $(\sigma-1)^p = (\tau-1)^p = 0$, so $(\tau-1)^{p-1}\alpha_L$ and $(\sigma-1)^{p-1}(\tau-1)^{p-2}\alpha_L$ are in X^G.

Suppose $(\sigma-1)^i(\tau-1)^j\alpha_L \in X\setminus\{0\}$ is neither of these. If $j=p-1$ then $i\neq 0$, so

$$(\sigma-1)^i(\tau-1)^j\alpha_L = (\sigma-1)^i(\tau-1)^{p-1}\alpha_L = (\sigma-1)^{i-1}(\tau-1)^p\alpha_R = 0,$$

a contradiction. Thus $j<p-1$, so

$$(\sigma-1)^{p-i-1}(\tau-1)^{p-j-2}(\sigma-1)^i(\tau-1)^j\alpha_L = (\sigma-1)^{p-1}(\tau-1)^{p-2}\alpha_L \neq 0$$

since at least one of $p-i-1$ and $p-j-2$ is nonzero. Hence $(\sigma-1)^i(\tau-1)^j\alpha_L \notin X^G$. □

Lemma 2.9. *Let X be an $\mathbb{F}_p[G]$-module with generators α_L and α_R satisfying $(\sigma-1)\alpha_L = (\tau-1)\alpha_R$ such that $(\tau-1)^{p-1}\alpha_L, (\sigma-1)^{p-1}(\tau-1)^{p-2}\alpha_L, (\sigma-1)^{p-1}\alpha_R \in X^G\setminus\{0\}$.*

Then $(\sigma-1)^i(\tau-1)^j\alpha_L = 0$ for $0\le i,j\le p-1$ if and only if $1\le i\le p-2$ and $j=p-1$. Similarly $(\sigma-1)^i(\tau-1)^j\alpha_R = 0$ if and only if $i=p-1$ and $1\le j\le p-2$.

Proof. If $1\le i\le p-2$, then $(\sigma-1)^i(\tau-1)^{p-1}\alpha_L = 0$ because $(\tau-1)^{p-1}\alpha_L$ is fixed by σ. We have $(\tau-1)^{p-1}\alpha_L \neq 0$ by assumption. If $1\le i\le p-1$ and $1\le j\le p-2$, then $(\sigma-1)^i(\tau-1)^j\alpha_L \neq 0$, else we would have

$$(\sigma-1)^{p-1}(\tau-1)^{p-2}\alpha_L = (\sigma-1)^{p-i-1}(\tau-1)^{p-j-2}(\sigma-1)^i(\tau-1)^j\alpha_L = 0$$

contradicting our hypotheses. □

According to Lemma 2.7, all elements in an $\mathbb{F}_p[G]$ module generated by α_L and α_R can be written as a sum of elements in the forms specified by Lemmas 2.8 and 2.9. Thus these lemmas can be used to identify the portions of such a sum that are trivial or fixed.

We will now show that the relation $(\sigma-1)\alpha_L = (\tau-1)\alpha_R$ and some specific linearly independent elements are sufficient to determine the structure of X. The idea of the proof is to assume that another relation exists, apply powers of $\sigma-1$ and/or $\tau-1$ until only known terms remain, and then contradict linear independence.

Theorem 2.10. *Let X be an $\mathbb{F}_p[G]$-module with generators α_L and α_R, let F be the free $\mathbb{F}_p[G]$-module with generators $\tilde{\alpha}_L$ and $\tilde{\alpha}_R$, and let $\iota : F \to X$ be the module homomorphism given by $\tilde{\alpha}_L \mapsto \alpha_L$ and $\tilde{\alpha}_R \mapsto \alpha_R$.*

If $(\sigma-1)\alpha_L = (\tau-1)\alpha_R$ and the elements $(\tau-1)^{p-1}\alpha_L$, $(\sigma-1)^{p-1}(\tau-1)^{p-2}\alpha_L$, and $(\sigma-1)^{p-1}\alpha_R$ are $\mathbb{F}_p$-linearly independent in X, then $\ker\iota = \langle(\sigma-1)\tilde{\alpha}_L - (\tau-1)\tilde{\alpha}_R\rangle$.

Proof. By hypothesis

$$\iota((\sigma-1)\tilde{\alpha}_L - (\tau-1)\tilde{\alpha}_R) = (\sigma-1)\alpha_L - (\tau-1)\alpha_R = 0$$

so $\langle(\sigma-1)\tilde{\alpha}_L - (\tau-1)\tilde{\alpha}_R\rangle \subseteq \ker\iota$. Suppose that $s \in \ker\iota$ for some $s \in F$. By Lemma 2.7 we can write

$$s = \sum_{i=0}^{p-1}\sum_{j=0}^{p-1}\beta_{ij}(\sigma-1)^i(\tau-1)^j\tilde{\alpha}_L + \sum_{i=0}^{p-1}\sum_{j=0}^{p-1}\gamma_{ij}(\sigma-1)^i(\tau-1)^j\tilde{\alpha}_R$$

for some $\beta_{ij}, \gamma_{ij} \in \mathbb{F}_p$. We have

$$\begin{aligned}\sum_{i=1}^{p-1}\sum_{j=0}^{p-2}\gamma_{ij}(\sigma-1)^i(\tau-1)^j\tilde{\alpha}_L - \sum_{i=0}^{p-2}\sum_{j=1}^{p-1}\gamma_{ij}(\sigma-1)^i(\tau-1)^j\tilde{\alpha}_R \\ = ((\sigma-1)\tilde{\alpha}_L - (\tau-1)\tilde{\alpha}_R)\sum_{i=0}^{p-2}\sum_{i=0}^{p-2}\gamma_{ij}(\sigma-1)^i(\tau-1)^j\end{aligned}$$

and since $(\sigma-1)^p = (\tau-1)^p = 0$ in $\mathbb{F}_p[G]$, we also have that

$$\begin{aligned}&\sum_{i=1}^{p-2}\beta_{i,p-1}(\sigma-1)^i(\tau-1)^{p-1}\tilde{\alpha}_L \\ &\qquad = \sum_{i=1}^{p-2}\beta_{i,p-1}(\sigma-1)^i(\tau-1)^{p-1}\tilde{\alpha}_L - \sum_{i=1}^{p-2}\beta_{i,p-1}(\sigma-1)^{i-1}(\tau-1)^p\tilde{\alpha}_R \\ &\qquad = ((\sigma-1)\tilde{\alpha}_L - (\tau-1)\tilde{\alpha}_R)\sum_{i=1}^{p-2}(\sigma-1)^{i-1}(\tau-1)^{p-1}\end{aligned}$$

and similarly

$$\sum_{i=1}^{p-2}\gamma_{p-1,j}(\sigma-1)^{p-1}(\tau-1)^j\tilde{\alpha}_R \in \langle(\sigma-1)\tilde{\alpha_L} - (\tau-1)\tilde{\alpha}_R\rangle.$$

Therefore, adding these, we have $s \in \langle(\sigma-1)\tilde{\alpha}_L - (\tau-1)\tilde{\alpha}_R\rangle$ if and only if

$$\sum_{j=1}^{p}\delta_{0j}(\tau-1)^{j-1}\tilde{\alpha}_L + \sum_{i=1}^{p-1}\sum_{j=1}^{p-1}\delta_{ij}(\sigma-1)^i(\tau-1)^{j-1}\tilde{\alpha}_L + \sum_{i=1}^{p}\delta_{i0}(\sigma-1)^{i-1}\tilde{\alpha}_R$$

is in the ideal, where $\delta_{0j} = \beta_{0,j-1}$, $\delta_{i0} = \gamma_{i-1,0}$, and $\delta_{ij} = \beta_{i,j-1} + \gamma_{i-1,j}$. We will show that $\delta_{ij} = 0$ for all i, j by contradiction. Note that the sums we added to s are also in $\ker \iota$, so this new element is as well, ie.

$$\sum_{j=1}^{p} \delta_{0j}(\tau-1)^{j-1}\alpha_L + \sum_{i=1}^{p-1}\sum_{j=1}^{p-1} \delta_{ij}(\sigma-1)^i(\tau-1)^{j-1}\alpha_L + \sum_{i=1}^{p} \delta_{i0}(\sigma-1)^{i-1}\alpha_R = 0.$$

Let m be the maximum index such that $\delta_{ij} = 0$ for all $0 \le i, j \le m-1$, and let n be the minimum index such that at least one of δ_{nm} and δ_{mn} is nonzero. Then $0 \le n \le m \le p$ with $m \neq 0$ and $n \neq p$. If $m = p$ then $n = 0$ so this relation is

$$\delta_{0p}(\tau-1)^{p-1}\alpha_L + \delta_{p0}(\sigma-1)^{p-1}\alpha_R = 0$$

where at least 1 of δ_{0p} and δ_{p0} is nonzero, and if $m = n = p-1$ then the relation is

$$\delta_{0p}(\tau-1)^{p-1}\alpha_L + \delta_{p-1,p-1}(\sigma-1)^{p-1}(\tau-1)^{p-2}\alpha_L + \delta_{p0}(\sigma-1)^{p-1}\alpha_R = 0$$

where $\delta_{p-1,p-1} \neq 0$. Both of these contradict our hypothesis of linear independence. We can thus assume that $0 \le n \le m \le p-1$ with $m \neq 0$ and $n \neq p-1$. Without loss of generality, suppose $\delta_{mn} \neq 0$.

Applying $(\sigma-1)^{p-m-1}(\tau-1)^{p-n-1}$ kills each term with at least one of $i \ge m+1$ and $j \ge n+1$ by Lemma 2.9 unless $m = p-1$, in which case a term with $i = 0$ and $j = n+1$ may also survive. The only nonzero coefficient δ_{ij} with $i \le m$ and $j \le n$ is δ_{mn} by choice of m and n. Thus the only terms remaining after application of $(\sigma-1)^{p-m-1}(\tau-1)^{p-n-1}$ are as follows:

case 1: $0 < m < p-1$ and $n > 0$

$$\begin{aligned} 0 &= (\sigma-1)^{p-m-1}(\tau-1)^{p-n-1}(\delta_{mn}(\sigma-1)^m(\tau-1)^{n-1}\alpha_L) \\ &= \delta_{mn}(\sigma-1)^{p-1}(\tau-1)^{p-2}\alpha_L \end{aligned}$$

case 2: $0 < m < p-1$ and $n = 0$

$$\begin{aligned} 0 &= (\sigma-1)^{p-m-1}(\tau-1)^{p-0-1}(\delta_{m0}(\sigma-1)^{m-1}\alpha_R) \\ &= \delta_{mn}(\sigma-1)^{p-2}(\tau-1)^{p-1}\alpha_R \\ &= \delta_{mn}(\sigma-1)^{p-1}(\tau-1)^{p-2}\alpha_L \end{aligned}$$

case 3: $m = p-1$ and $0 < n < p-1$

$$\begin{aligned} 0 &= (\sigma-1)^{p-(p-1)-1}(\tau-1)^{p-n-1}(\delta_{mn}(\sigma-1)^{p-1}(\tau-1)^{n-1}\alpha_L + \delta_{0,n+1}(\tau-1)^n\alpha_L) \\ &= \delta_{mn}(\sigma-1)^{p-1}(\tau-1)^{p-2}\alpha_L + \delta_{0,n+1}(\tau-1)^{p-1}\alpha_L \end{aligned}$$

case 4: $m = p-1$ and $n = 0$

$$\begin{aligned} 0 &= (\sigma-1)^{p-(p-1)-1}(\tau-1)^{p-0-1}(\delta_{mn}(\sigma-1)^{p-2}\alpha_R + \delta_{01}(\tau-1)^0\alpha_L) \\ &= \delta_{mn}(\sigma-1)^{p-2}(\tau-1)^{p-1}\alpha_R + \delta_{01}(\tau-1)^{p-1}\alpha_L \\ &= \delta_{mn}(\sigma-1)^{p-1}(\tau-1)^{p-2}\alpha_L + \delta_{01}(\tau-1)^{p-1}\alpha_L \end{aligned}$$

In each case $\delta_{mn} \neq 0$, contradicting linear independence. Therefore no such δ_{mn} exists, so $s \in \langle(\sigma-1)\tilde{\alpha_L} - (\tau-1)\tilde{\alpha}_R\rangle$.

□

Corollary 2.11. *If X is as given in Theorem 2.10, then the union of the sets*

$$\{(\tau-1)^j\alpha_L : 0 \leq j \leq p-1\}$$
$$\{(\sigma-1)^i(\tau-1)^j\alpha_L : 1 \leq i \leq p-1, 0 \leq j \leq p-2\}$$
$$\{(\sigma-1)^i\alpha_R : 0 \leq i \leq p-1\}$$

is an $\mathbb{F}_p$-basis for X.

Proof. Independence follows from the previous proof and spanning from Lemma 2.7. □

Corollary 2.12. *If X is as given in Theorem 2.10, then*

$$X^G = \left\langle (\tau-1)^{p-1}\alpha_L, (\sigma-1)^{p-1}(\tau-1)^{p-2}\alpha_L, (\sigma-1)^{p-1}\alpha_R \right\rangle_{\mathbb{F}_p}.$$

Proof. Suppose $x \in X^G$. Then by Corollary 2.11 there exist $\delta_{ij} \in \mathbb{F}_p$ such that

$$x = \sum_{j=1}^{p} \delta_{0j}(\tau-1)^{j-1}\alpha_L + \sum_{i=1}^{p-1}\sum_{j=1}^{p-1} \delta_{ij}(\sigma-1)^i(\tau-1)^{j-1}\alpha_L + \sum_{i=1}^{p} \delta_{i0}(\sigma-1)^{i-1}\alpha_R.$$

Then $(\tau-1)x = 0$ and $(\sigma-1)x = 0$ so by Corollary 2.11 the coefficient corresponding to each term that is not fixed is 0. This leaves

$$x = \delta_{0p}(\tau-1)^{p-1}\alpha_L + \delta_{p-1,p-1}(\sigma-1)^{p-1}(\tau-1)^{p-2}\alpha_L + \delta_{p0}(\sigma-1)^{p-1}\alpha_R$$

by Lemma 2.8 so x is in the desired span. The converse also follows from Lemma 2.8. □

Finally, we will prove that X is indecomposable, with the help of a strange but useful lemma.

Lemma 2.13. *Let X be the $\mathbb{F}_p[\mathrm{Gal}(K/F)]$-module X generated by α_L and α_R subject to the relation $(\sigma-1)\alpha_L = (\tau-1)\alpha_R$. If $x \in X$ with $(\tau-1)x, (\sigma-1)^{p-1}x \in X^G$ then either $(\sigma-1)^{p-1}x = 0$ or they are linearly independent.*

Similarly, if $(\sigma-1)x, (\tau-1)^{p-1}x \in X^G$ then either $(\tau-1)^{p-1}x = 0$ or they are independent.

Proof. By Corollary 2.12, there exist $\delta_1, \delta_2, \delta_3, \gamma_1, \gamma_2, \gamma_3 \in \mathbb{F}_p$ such that

$$(\tau-1)x = \delta_1(\tau-1)^{p-1}\alpha_L + \delta_2(\sigma-1)^{p-2}(\tau-1)^{p-1}\alpha_R + \delta_3(\sigma-1)^{p-1}\alpha_R$$

and

$$(\sigma-1)^{p-1}x = \gamma_1(\tau-1)^{p-1}\alpha_L + \gamma_2(\sigma-1)^{p-1}(\tau-1)^{p-2}\alpha_L + \gamma_3(\sigma-1)^{p-1}\alpha_R.$$

Thus $\delta_3(\sigma-1)^{p-1}\alpha_R$ is in the image of $\tau-1$. However $(\sigma-1)^{p-1}\alpha_R$ is not, so we must have $\delta_3 = 0$. Similarly $\gamma_1(\tau-1)^{p-1}\alpha_L$ is in the image of $\sigma-1$ but $(\tau-1)^{p-1}\alpha_L$ is not, so $\gamma_1 = 0$. Then

$$(\tau-1)x = (\tau-1)(\delta_1(\tau-1)^{p-2}\alpha_L + \delta_2(\sigma-1)^{p-2}(\tau-1)^{p-2}\alpha_R)$$

so there exists $y \in \ker(\tau - 1)$ such that

$$x = \delta_1(\tau-1)^{p-2}\alpha_L + \delta_2(\sigma-1)^{p-2}(\tau-1)^{p-2}\alpha_R + y.$$

By Corollary 2.11 we can write y as an $\mathbb{F}_p$-combination of $(\sigma-1)^{p-1}\alpha_R$ and the terms $(\sigma-1)^i(\tau-1)^j\alpha_L$ that are in $\ker(\tau-1)$ according to Lemma 2.9, all of which are also in $\ker(\sigma-1)^{p-1}$, so $(\sigma-1)^{p-1}y = 0$ and thus

$$\begin{aligned}\delta_1(\sigma-1)^{p-1}(\tau-1)^{p-2}\alpha_L &= (\sigma-1)^{p-1}x \\ &= \gamma_2(\sigma-1)^{p-1}(\tau-1)^{p-2}\alpha_L + \gamma_3(\sigma-1)^{p-1}\alpha_R.\end{aligned}$$

Hence by linear independence we have $\gamma_3 = 0$ and $\gamma_2 = \delta_1$.

case 1: $\gamma_2 = \delta_1 = 0$

Then $\gamma_1 = \gamma_2 = \gamma_3 = 0$, so $(\sigma-1)^{p-1}x = 0$.

case 2: $\gamma_2 = \delta_1 \neq 0$

Then

$$\begin{aligned}(\tau-1)x &= \delta_1(\tau-1)^{p-1}\alpha_L + \delta_2(\sigma-1)^{p-2}(\tau-1)^{p-1}\alpha_R \\ &= \delta_1(\tau-1)^{p-1}\alpha_L + \delta_2(\sigma-1)^{p-1}(\tau-1)^{p-2}\alpha_L \\ (\sigma-1)^{p-1}x &= \delta_1(\sigma-1)^{p-1}(\tau-1)^{p-2}\alpha_L\end{aligned}$$

where $\delta_1 \neq 0$, so $(\tau-1)x$ and $(\sigma-1)^{p-1}x$ are linearly independent because $(\tau-1)^{p-1}\alpha_L$ and $(\sigma-1)^{p-2}(\tau-1)^{p-1}\alpha_R$ are.

These give the 2 cases in the lemma. □

Theorem 2.14. *An $\mathbb{F}_p[G]$-module X with generators α_L and α_R that satisfy $(\sigma-1)\alpha_L = (\tau-1)\alpha_R$ such that $(\sigma-1)^{p-1}\alpha_L$, $(\sigma-1)^{p-1}(\tau-1)^{p-2}\alpha_L$, and $(\sigma-1)^{p-1}\alpha_R$ are $\mathbb{F}_p$-linearly independent is indecomposable.*

Proof. Suppose $X = A \oplus B$ for some submodules A and B.

case 1: $A^G = A$

Since $\alpha_L \in X$, there exist $\alpha_A \in A$ and $\alpha_B \in B$ such that $\alpha_L = \alpha_A + \alpha_B$. Thus

$$(\tau-1)^{p-1}\alpha_L = (\tau-1)^{p-1}(\alpha_A + \alpha_B) = 0 + (\tau-1)^{p-1}\alpha_B \in B$$

and

$$(\sigma-1)^{p-1}(\tau-1)^{p-2}\alpha_L = 0 + (\sigma-1)^{p-1}(\tau-1)^{p-2}\alpha_B \in B.$$

Applying the same reasoning to α_R gives

$$(\sigma-1)^{p-1}\alpha_R \in B$$

so $\dim_{\mathbb{F}_p} B^G = 3$.

case 2: $A^G \neq A$

Let $x \in A \setminus A^G$, let i be the maximum index such that $(\sigma-1)^i x \neq 0$, and let j be the maximum index such that $(\sigma-1)^i(\tau-1)^j x \neq 0$. Then $(\sigma-1)^i(\tau-1)^j x \in A^G$ and at least one of i and j is nonzero.

Without loss of generality, suppose $j \neq 0$. Let $\delta_1, \delta_2, \delta_3 \in \mathbb{F}_p$ such that

$$(\sigma-1)^i(\tau-1)^j x = \delta_1(\tau-1)^{p-1}\alpha_L + \delta_2(\sigma-1)^{p-2}(\tau-1)^{p-1}\alpha_R + \delta_3(\sigma-1)^{p-1}\alpha_R$$

(possible by Corollary 2.12). Then $\delta_3(\sigma-1)^{p-1}\alpha_R$ is in the image of $\tau-1$ while $(\sigma-1)^{p-1}\alpha_R$ is not, so $\delta_3 = 0$.

subcase a: $\delta_1 \neq 0$

Then $i = 0$, else $(\tau-1)^{p-1}\alpha_L$ is in the image of $\sigma-1$. Write

$$(\tau-1)^{j-1}x = x_A + x_B$$

for $x_A \in A$ and $x_B \in B$. Then $(\tau-1)x_A + (\tau-1)x_B = (\tau-1)^j x \in A$ with $(\tau-1)x_A \in A$ and $(\tau-1)x_B \in B$, so $(\tau-1)x_B = 0$ and thus $(\tau-1)x_A = (\tau-1)^j x$, which has $\delta_1 \neq 0$. Thus we are in case 2 of the proof of Lemma 2.13, so $(\sigma-1)^{p-1}x_A$ is independent from $(\tau-1)x_A$.

subcase b: $\delta_1 = 0$

Then $(\sigma-1)^i(\tau-1)^j x = \delta_2(\sigma-1)^{p-1}(\tau-1)^{p-2}\alpha_L$ with $\delta_2 \neq 0$. Write

$$\delta_2(\tau-1)^{p-2}\alpha_L = x_A + x_B$$

for $x_A \in A$ and $x_B \in B$. Then $(\sigma-1)^{p-1}x_A + (\sigma-1)^{p-1}x_B \in A$ so

$$(\sigma-1)^{p-1}x_A = \delta_2(\sigma-1)^{p-1}(\tau-1)^{p-2}\alpha_L \neq 0$$

as above. Thus $(\tau-1)x_A$ is independent from $(\sigma-1)^{p-1}x_A$ by Lemma 2.13.

In either subcase $\dim_{\mathbb{F}_p} A^G \geq 2$.

We have

$$3 \geq \dim_{\mathbb{F}_p} X^G = \dim_{\mathbb{F}_p}(A \oplus B)^G = \dim_{\mathbb{F}_p} A^G \oplus B^G = \dim_{\mathbb{F}_p} A^G + \dim_{\mathbb{F}_p} B^G$$

by Corollary 2.12 and Lemma 2.6. Case 1 gives that $\dim_{\mathbb{F}_p} A^G = 0$, which implies $A = 0$ by Lemma 2.5, so that $A \oplus B$ is trivial. If neither A nor B is trivial then they both fall under case 2, so $\dim_{\mathbb{F}_p} A^G, \dim_{\mathbb{F}_p} B^G \geq 2$, a contradiction. □

Chapter 3

Klein 4-group case

This chapter will present the decomposition of $K^+/\wp(K)$ as an $\mathbb{F}_2[\mathrm{Gal}(K/F)]$-module when $\mathrm{Gal}(K/F) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. This case is slightly different from the general one due to peculiarities of $p = 2$, but the methods used are nonetheless similar.

3.1 Notation

Let K/F be a Galois field extension of characteristic 2 with

$$\mathrm{Gal}(K/F) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} = \langle \sigma, \tau \rangle .$$

Call the intermediate fields of this extension K_1, K_2, and K_3, and let $\theta_a, \theta_b \in K$ such that

$$\begin{aligned} K_1 &= F(\theta_a) = \mathrm{Fix}\,\langle \tau \rangle \\ K_2 &= F(\theta_b) = \mathrm{Fix}\,\langle \sigma \rangle \\ K_3 &= F(\theta_{a+b} = \theta_a + \theta_b) = \mathrm{Fix}\,\langle \sigma\tau \rangle . \end{aligned}$$

Then $K = F(\theta_a, \theta_b)$ and the minimum polynomials of θ_a and θ_b over F have the forms $x^2 - x - a$ and $x^2 - x - b$, respectively, for some $a, b \in F$. Thus we can choose the generators σ and τ so that

$$\begin{aligned} \sigma(\theta_a) &= \theta_a + 1 \\ \tau(\theta_b) &= \theta_b + 1. \end{aligned}$$

For an intermediate field M define the normal subgroup

$$\wp(M) = \{m^2 - m : m \in M\}$$

of M^+, the group of M under addition. We will write cosets as follows:

$$\begin{aligned} [f] &= f + \wp(K) \\ [f]_{K_1} &= f + \wp(K_1) \\ [f]_{K_2} &= f + \wp(K_2) \\ [f]_{K_3} &= f + \wp(K_3) \end{aligned}$$

In particular let

$$J = K^+/\wp(K)$$

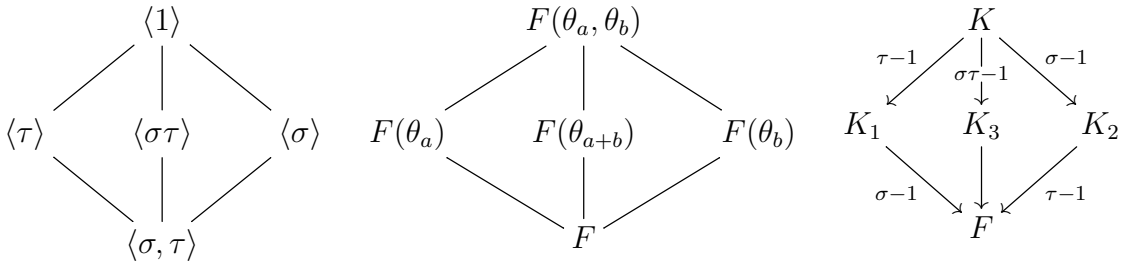
and

$$J^G = \{[k] \in J : [\sigma(k)] = [k] = [\tau(k)]\}.$$

We will indicate the $\mathbb{F}_2[\mathrm{Gal}(K/F)]$-span of $[k]$ by $\langle [k] \rangle$ and the $\mathbb{F}_2$-span by $\langle [k] \rangle_{\mathbb{F}_2}$. For a subfield M of K let

$$[M] = \{[m] \in J : m \in M\}.$$

For reference, here is a subgroup lattice for $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ with the corresponding fixed fields and trace maps:



Note that $\sigma - 1 = \sigma + 1$ and $\tau - 1 = \tau + 1$ in characteristic 2. We choose to write the former from analogy with the general case. As expected, we also have $T_{K/F} = \sigma\tau + \sigma + \tau = (\sigma - 1)(\tau - 1) = T_{K_1/F} \circ T_{K/K_1}$ and similarly $T_{K/F} = T_{K_2/F} \circ T_{K/K_2}$. Where it does not create confusion, we may write T_{K/K_2} for $T_{K_1/F}$ and T_{K/K_1} for $T_{K_2/F}$.

3.2 The map T

Since K/F has 3 intermediate fields, we can classify elements of J by their images under trace maps by combining them into a single function. Restricting the domain to J^G allows us to enumerate the possible outputs.

Definition 3. Let

$$T\colon J^G \to \frac{K_1^+}{\wp(K_1)} \times \frac{K_2^+}{\wp(K_2)} \times \frac{K_3^+}{\wp(K_3)}$$

be given by

$$T([k]) = \left([T_{K/K_1}(k)]_{K_1}, [T_{K/K_2}(k)]_{K_2}, [T_{K/K_3}(k)]_{K_3}\right).$$

This T will be fixed for the remainder of Chapter 3, and we will not include class notation when writing images. Note that it is a homomorphism because the T_{K/K_i} are.

Lemma 3.1. *If $k_2 \in K_2$ with $[k_2] = [0]$, then there exists $\ell \in \mathbb{F}_2$ such that $[k_2]_{K_2} = [\ell a]_{K_2}$.*

Proof. Let U be the subgroup of $K_2^+/\wp(K_2)$ generated by $[a]_{K_2}$. We will first show that

$$K = K_2(\theta_{k_2} : [k_2]_{K_2} \in U)$$

where θ_{k_2} is a root of the polynomial $x^2 - x - k_2$. Since $[a]_{K_2} \in U$, we have

$$K = K_2(\theta_a) \subseteq K_2(\theta_{k_2} : [k_2]_{K_2} \in U).$$

Suppose $[k_2] \in U$. By definition of U there exists $\ell \in \mathbb{F}_2$ such that $[k_2]_{K_2} = [\ell a]_{K_2}$. We have

$$(\ell\theta_a)^2 - \ell\theta_a = \ell(\theta_a^2 - \theta_a) = \ell a$$

so there exists $z \in \mathbb{F}_2$ such that $\theta_{k_2} = \theta_a + z$. Thus $\theta_{k_2} \in K(\theta_a)$, so

$$K_2(\theta_{k_2} : [k_2]_{K_2} \in U) \subseteq K(\theta_a) = K.$$

Hence by Theorem 1.2

$$U = \{[k_2]_{K_2} : k_2 \in K_2 \cap \wp(K)\}$$

so $k_2 \in K_2$ and $[k_2] = 0$ implies that there exists $\ell \in \mathbb{F}_2$ such that $[k_2] = [\ell a]$. □

Similarly $k_1 \in K_1 \cap \wp(K)$ implies $[k_1]_{K_1} = [\ell b]_{K_1}$ for some $\ell \in \mathbb{F}_2$, and $k_3 \in K_3$ implies $[k_3]_{K_3} = [\ell a]_{K_3} = [\ell b]_{K_3}$ for some $\ell \in \mathbb{F}_2$. (One can see that $[a]_{K_3} = [b]_{K_3}$ because $[a+b]_{K_3} = [0]_{K_3}$.) For $[k] \in J^G$ we have

$$[T_{K/K_1}(k)] = [T_{K/K_2}(k)] = [T_{K/K_3}(k)] = [0]$$

so all possibilities for $T([k])$ are listed below:

$$\begin{array}{cccc} (0,0,0) & (0,0,a) & (b,0,0) & (b,0,a) \\ (0,a,0) & (0,a,a) & (b,a,0) & (b,a,a) \end{array}$$

The kernel of T is precisely the classes in J with at least one representative in the ground field F, which will be extremely useful when constructing our decomposition. The type of extension problem involved in the proof is described more thoroughly in Section 4.2.

Theorem 3.2. $\ker T = [F]$.

Proof. Since F is fixed by σ and τ we have $[F] \subseteq \ker T$. Let $[\gamma] \in \ker T$, let θ_γ be a root of the polynomial $x^2 - x - \gamma$, let $L = K(\theta_\gamma)$, and let $\tilde{\mu}$ be a generator for $\mathrm{Gal}(L/K)$ as a subgroup of $\mathrm{Gal}(L/F)$. Then $\mathrm{Gal}(L/F)$ has order 8 and $\mathrm{Gal}(K/F) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ as a quotient, so $\mathrm{Gal}(L/F)$ is isomorphic to exactly one of the following:

$$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \qquad \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \qquad D_8 \qquad Q_8$$

(where D_8 and Q_8 are the dihedral group on 8 elements and the quaternions, respectively). Denote by $\tilde{\sigma}$ and $\tilde{\tau}$ lifts of σ and τ in $\mathrm{Gal}(L/F)$, respectively. Since $[T_{K/K_1}(\gamma)]_{K_1} = [0]_{K_1}$ we have

$$k_1^2 - k_1 = T_{K/K_1}(\gamma) = (\tilde{\tau} - 1)\gamma$$

for some $k_1 \in K_1$. We also have

$$((\tilde{\tau} - 1)\theta_\gamma)^2 - (\tilde{\tau} - 1)\theta_\gamma = (\tilde{\tau} - 1)(\theta_\gamma^2 - \theta_\gamma) = (\tilde{\tau} - 1)\gamma$$

so k_1 and $(\tilde{\tau} - 1)\theta_\gamma$ are roots of the same Artin-Schreier polynomial. Thus $(\tilde{\tau} - 1)\theta_\gamma = k_1 + z$ for some $z \in \mathbb{F}_2$, so

$$(\tilde{\tau}^2 - 1)\theta_\gamma = (\tilde{\tau} + 1)(\tilde{\tau} - 1)\theta_\gamma = (\tilde{\tau} + 1)(k_1 + z) = k_1 + z + k_1 + z = 0.$$

Since $\tilde{\tau}^2$ fixes θ_a and θ_b, this gives $\tilde{\tau}^2 = 1$. Similarly $\tilde{\sigma}^2 = 1$ because $[T_{K/K_2}(\gamma)]_{K_2} = [0]_{K_2}$.

If $\mathrm{Gal}(L/F) \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ then $\tilde{\mu}$, $\tilde{\sigma}$, and $\tilde{\tau}$ are distinct and all have order 2, so they are equal to $(0,1)$, $(2,0)$, and $(2,1)$ in some order. Only $\tilde{\mu} = (2,0)$ gives the quotient $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$. However $(0,1) = (2,1)$ modulo $\langle(2,2)\rangle$. Therefore $\mathrm{Gal}(L/F) \ncong \mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$.

There is only 1 element of order 2 in Q_8, namely -1, so $\mathrm{Gal}(L/F) \ncong Q_8$.

Since $[T_{K/K_3}(\gamma)]_{K_3} = [0]_{K_3}$ there exists $k_3 \in K_3$ such that $k_3^2 - k_3 = (\tilde{\sigma}\tilde{\tau} - 1)\gamma$. Then there exists $z' \in \mathbb{F}_2$ such that $(\tilde{\sigma}\tilde{\tau} - 1)\theta_\gamma = k_3 + z'$ as before. Since $\tilde{\sigma}$ and $\tilde{\tau}$ have order 2, they are their own inverses. Thus

$$\begin{aligned}
([\tilde{\sigma}, \tilde{\tau}] - 1)\theta_\gamma &= (\tilde{\sigma}\tilde{\tau}\tilde{\sigma}^{-1}\tilde{\tau}^{-1} - 1)\theta_\gamma \\
&= ((\tilde{\sigma}\tilde{\tau})^2 - 1)\theta_\gamma \\
&= (\tilde{\sigma}\tilde{\tau} + 1)(\tilde{\sigma}\tilde{\tau} - 1)\theta_\gamma \\
&= (\tilde{\sigma}\tilde{\tau} + 1)(k_3 + z') \\
&= k_3 + z' + k_3 + z' \\
&= 0
\end{aligned}$$

so $[\tilde{\sigma}, \tilde{\tau}] = 1$ because it fixes θ_a and θ_b.

If $\mathrm{Gal}(L/F) \cong D_8$ then $\tilde{\mu}$ generates the center, the only normal subgroup of order 2. However there are no elements of order 2 in D_8 that commute with each other and are distinct modulo the center. Therefore $\mathrm{Gal}(L/F) \ncong D_8$, so $\mathrm{Gal}(L/F) \cong \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$.

By Theorem 1.2 there exist $\gamma_1, \gamma_2, \gamma_3 \in F$ such that $L = F(\theta_{\gamma_1}, \theta_{\gamma_2}, \theta_{\gamma_3})$. Since $F(\theta_a)$ and $F(\theta_b)$ are distinct subfields of L, we can take $\gamma_1 = a$ and $\gamma_2 = b$. This gives $K(\theta_\gamma) = L = K(\theta_{\gamma_3})$, so $[\gamma]$ is an element of the subgroup generated by $[\gamma_3]$ in $K^+/\wp(K)$. Since $[\gamma_3] \in [F]$, we must have $[\gamma] \in [F]$. □

3.3 Construction of Y

Since $[F]$ is fixed by $\mathrm{Gal}(K/F)$, it is a vector space over $\mathbb{F}_2$, so linear algebra guarantees the existence of a set of elements spanning it. Since $T_{K/F}$ is surjective we can take preimages of these elements in order to construct a larger submodule whose components are free $\mathbb{F}_2[\mathrm{Gal}(K/F)]$-modules with fixed parts in $[F]$.

Definition 4. Let $\mathcal{I}$ be a basis for $[F]$ as an $\mathbb{F}_2$ vector space, and for each $[y] \in \mathcal{I}$ choose $k_\ell \in K$ such that $T_{K/F}(k_y) = y$. (Such a k_y exists by Corollary 2.4.) Define Y to be the $\mathbb{F}_2[\mathrm{Gal}(K/F)]$-span of the classes of these elements in J:

$$Y = \sum_{[y]\in\mathcal{I}} \langle [k_y] \rangle$$

Theorem 3.3. *If $[y_1], [y_2] \in \mathcal{I}$ and $[y_1] \neq [y_2]$, then $\langle [k_{y_1}] \rangle \cap \langle [k_{y_2}] \rangle = \{[0]\}$.*

Proof. We will show that the fixed part of $\langle [k_{y_1}] \rangle$ is the $\mathbb{F}_2$-span of $[y_1]$. Since $[y_1] \in [F] \cap \langle [k_{y_1}] \rangle$ we have $\langle [y_1] \rangle_{\mathbb{F}_2} \subseteq \langle [k_{y_1}] \rangle^G$. Conversely, let $[y] \in \langle [k_{y_1}] \rangle^G$. By Lemma 2.7

$$y = (\alpha_1 + \alpha_2(\sigma - 1) + \alpha_3(\tau - 1) + \alpha_4(\sigma - 1)(\tau - 1))k_{y_1}$$

for some $\alpha_1, \ldots, \alpha_4 \in \mathbb{F}_2$ and by hypothesis

$$[0] = (\sigma - 1)[y] = (\alpha_1(\sigma - 1) + \alpha_3(\sigma - 1)(\tau - 1))[k_{y_1}] = \alpha_1 T_{K/K_2}[k_{y_1}] + \alpha_3[y_1]$$

and

$$[0] = (\tau - 1)[y] = (\alpha_1(\tau - 1) + \alpha_2(\sigma - 1)(\tau - 1))[k_{y_1}] = \alpha_1 T_{K/K_1}[k_{y_1}] + \alpha_2[y_1]$$

where $\alpha_2[y_1], \alpha_3[y_1] \in [F]$. However $T_{K/K_1}[k_{y_1}]$ or $T_{K/K_2}[k_{y_1}]$ in $[F]$ would imply $[y_1] = T_{K/F}[k_{y_1}] = T_{K/K_1} \circ T_{K/K_2}[k_{y_1}] = [0]$, which is not true by linear independence of $\mathfrak{I}$. Therefore $\alpha_1 = \alpha_2 = \alpha_3 = 0$, so

$$[y] = \alpha_4(\sigma - 1)(\tau - 1)[k_{y_1}] = \alpha_4[y_1] \in \langle [y_1] \rangle_{\mathbb{F}_2}$$

and thus $\langle [k_{y_1}] \rangle^G = \langle [y_1] \rangle_{\mathbb{F}_2}$ and $\langle [k_{y_2}] \rangle^G = \langle [y_2] \rangle_{\mathbb{F}_2}$.

We also have $\langle [y_1] \rangle_{\mathbb{F}_2} \cap \langle [y_2] \rangle_{\mathbb{F}_2} = \{[0]\}$ by linear independence, so $\langle [k_{y_1}] \rangle \cap \langle [k_{y_2}] \rangle = \{[0]\}$ by Lemma 2.5. □

Therefore

$$Y = \bigoplus_{[y] \in \mathfrak{I}} \langle [k_y] \rangle .$$

This module will be fixed for the remainder of Chapter 3.

Corollary 3.4. $Y^G = [F]$.

Proof. This follows from the fact that $\langle [k_y] \rangle^G = \langle [y] \rangle_{\mathbb{F}_2}$ for each $[y] \in \mathfrak{I}$ where $\mathfrak{I}$ spans $[F]$. □

3.4 Construction of X

According to Corollary 3.4 and Theorem 3.2, our decomposition so far only covers the kernel of T. To have any hope of spanning J^G we must at least include one class $[x] \in J^G$ with $T([x]) \neq (0, 0, 0)$, and the largest submodule would arise if $[x]$ were in the image of both T_{K/K_1} and T_{K/K_2}. (For our purposes this is equivalent to $[x] \in [K_1] \cap [K_2]$, but we state the following theorem this way to correspond to the first case of Proposition 7 in [1].)

Theorem 3.5. $T([T_{K/K_1}(K)] \cap [T_{K/K_2}(K)] \cap J^G) \neq \{(0, 0, 0)\}$

Proof. Consider $b\theta_a + a\theta_b \in K$. Since

$$T([b\theta_a + a\theta_b]) = (a, b, a + b) = (0, 0, 0)$$

there exists $c \in F$ such that

$$[b\theta_a + a\theta_b] = [c]$$

by Theorem 3.2 and thus

$$[c + b\theta_a] = [a\theta_b].$$

Call this equivalence class $[x]$. We have

$$\sigma([x]) = [\sigma(a\theta_b)] = [a\theta_b] = [x]$$
$$\tau([x]) = [\tau(c + b\theta_a)] = [c + b\theta_a] = [x]$$

so $[x] \in J^G$. Furthermore

$$[x] = [c + b\theta_a] \in [K_1] = [T_{K/K_1}(K)]$$
$$[x] = [a\theta_b] \in [K_2] = [T_{K/K_2}(K)]$$

by Corollary 2.4. Therefore

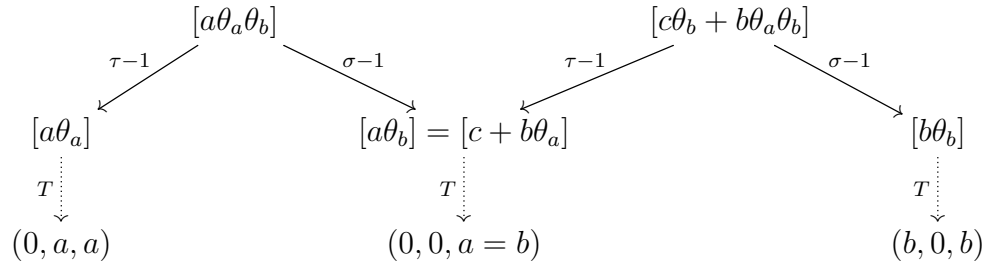
$$[x] \in [T_{K/K_1}(K)] \cap [T_{K/K_2}(K)] \cap J^G$$

with

$$T([x]) = (a, b, a) = (0, 0, a) \neq (0, 0, 0)$$

as desired. □

Now we use the fact that $[x]$ is in the image of T_{K/K_1} and T_{K/K_2} to construct a submodule containing it, to be fixed for the remainder of Chapter 3. By taking explicit preimages, we obtain the 2 generators at the top of the following diagram:



Note that the location of c on the right hand side of this diagram and not the left is arbitrary.

Definition 5. Let $c \in F$ be as given in the proof of Theorem 3.5, and define X to be the $\mathbb{F}_2[\mathrm{Gal}(K/F)]$-span of the classes of $a\theta_a\theta_b$ and $c\theta_b + b\theta_a\theta_b$ in J:

$$X = \langle [a\theta_a\theta_b], [c\theta_b + b\theta_a\theta_b] \rangle$$

This X will be fixed for the remainder of Chapter 3.

We now show that X is the module described in Section 2.2, from which some properties immediately follow.

Theorem 3.6. *The classes $[a\theta_a]$, $[a\theta_b] = [c + b\theta_a]$, and $[b\theta_b]$ are $\mathbb{F}_2$-linearly independent.*

Proof. Suppose $\delta_1[a\theta_a] + \delta_2[a\theta_b] + \delta_3[b\theta_b] = [0]$ for some $\delta_1, \delta_2, \delta_3 \in \mathbb{F}_2$. Then

$$\begin{aligned}(0, 0, 0) &= T([0]) \\ &= T(\delta_1[a\theta_a] + \delta_2[a\theta_b] + \delta_3[b\theta_b]) \\ &= \delta_1 T([a\theta_a]) + \delta_2 T([a\theta_b]) + \delta_3 T([b\theta_b]) \\ &= \delta_1(0, a, a) + \delta_2(0, 0, a) + \delta_3(b, 0, a)\end{aligned}$$

so $\delta_1 = \delta_2 = \delta_3 = 0$. □

Corollary 3.7. *The submodule X is indecomposable.*

Proof. Take $\alpha_L = [a\theta_a\theta_b]$ and $\alpha_R = [c\theta_b + b\theta_a\theta_b]$ in Theorem 2.14. □

Corollary 3.8. $X^G = \langle [a\theta_a], [a\theta_b], [b\theta_b] \rangle_{\mathbb{F}_2}$.

Proof. Take $\alpha_L = [a\theta_a\theta_b]$ and $\alpha_R = [c\theta_b + b\theta_a\theta_b]$ in Corollary 2.12. □

3.5 Structure of J

Theorem 3.9. *If $X = \langle [a\theta_a\theta_b], [c\theta_b + b\theta_a\theta_b] \rangle$ and $Y = \bigoplus_{[y]\in\mathcal{J}} \langle [k_y] \rangle$ as defined above, then*

$$J = X \oplus Y.$$

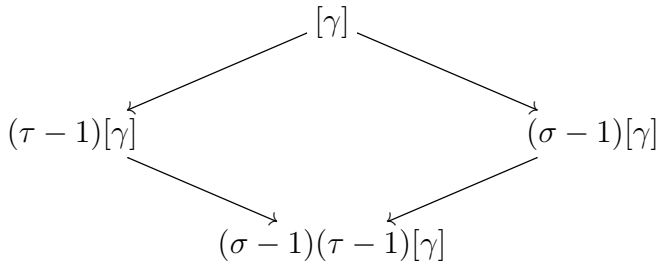
Lemma 3.10. $J^G = X^G + Y^G$

Proof. Clearly $X^G + Y^G \subseteq J^G$. Suppose $[\gamma] \in J^G$ and let $\ell_1, \ell_2, \ell_3 \in \mathbb{F}_2$ such that $T([\gamma]) = (\ell_1 b, \ell_2 a, \ell_3 a)$, which is possible by Lemma 3.1. Then

$$\begin{aligned} &T([\gamma + \ell_2 a\theta_a + (\ell_3 + \ell_2 + \ell_1)a\theta_b + \ell_1 b\theta_b]) \\ &\quad = T([\gamma]) + \ell_2 T([a\theta_a]) + (\ell_3 + \ell_2 + \ell_1)T([a\theta_b]) + \ell_1 T([b\theta_b]) \\ &\quad = (\ell_1 b, \ell_2 a, \ell_3 a) + \ell_2(0, a, a) + (\ell_3 + \ell_2 + \ell_1)(0, 0, a) + \ell_1(b, 0, a) \\ &\quad = (0, 0, 0) \end{aligned}$$

so $[\gamma + \ell_2 a\theta_a + (\ell_3 + \ell_2 + \ell_1)a\theta_b + \ell_1 b\theta_b] \in [F] = Y^G$ by Theorem 3.2 and Corollary 3.4. Since $\ell_2 a\theta_a + (\ell_3 + \ell_2 + \ell_1)a\theta_b + \ell_1 b\theta_b \in X^G$ by Corollary 3.8 this gives $[\gamma] \in X^G + Y^G$. □

If $[\gamma] \in J$, then $[\gamma]$ generates up to 3 additional classes after application of $\sigma - 1$ and $\tau - 1$:



We will show that $[\gamma] \in X \oplus Y$ by repeatedly adding terms to $[\gamma]$ in order to reduce the number of nonzero entries in this diagram.

Lemma 3.11. *If $(\tau - 1)[\gamma] = [0]$, then $T((\sigma - 1)[\gamma]) = (0, 0, 0)$.*

Proof. Since $[(\sigma - 1)\gamma] \in [K_2]$ we have $[T_{K/K_2}((\sigma - 1)\gamma)]_{K_2} = [0]_{K_2}$. Since $(\tau - 1)[\gamma] = [0]$ there are 2 cases for $[T_{K/K_1}((\sigma - 1)\gamma)]_{K_1}$ according to Lemma 3.1:

case 1: $[(\tau - 1)\gamma]_{K_1} = [0]_{K_1}$

$$\begin{aligned} [T_{K/K_1}((\sigma - 1)\gamma)]_{K_1} &= [(\tau - 1)(\sigma - 1)\gamma]_{K_1} \\ &= (\sigma - 1)[(\tau - 1)\gamma]_{K_1} \\ &= (\sigma - 1)[0]_{K_1} \\ &= [0]_{K_1} \end{aligned}$$

case 2: $[(\tau-1)\gamma]_{K_1} = [b]_{K_1}$

$$\begin{aligned}[T_{K/K_1}((\sigma-1)\gamma)]_{K_1} &= (\sigma-1)[b]_{K_1} \\ &= [b]_{K_1} - [b]_{K_1} \\ &= [0]_{K_1}\end{aligned}$$

In either case $[T_{K/K_1}((\sigma-1)\gamma)]_{K_1} = [0]_{K_1}$. We will show that $[T_{K/K_3}((\sigma-1)\gamma)]_{K_3} = [0]_{K_3}$ by contrapositive. Suppose $[T_{K/K_3}((\sigma-1)\gamma)]_{K_3} \neq [0]_{K_3}$. Then

$$\begin{aligned}[0]_{K_3} &\neq [T_{K/K_3}((\sigma-1)\gamma)]_{K_3} \\ &= [(\sigma\tau-1)(\sigma-1)\gamma]_{K_3} \\ &= [(\sigma^2\tau-\sigma\tau-\sigma+1)\gamma]_{K_3} \\ &= [(\tau-\sigma\tau-\sigma\tau^2+1)\gamma]_{K_3} \\ &= [(\sigma\tau^2-\sigma\tau-\tau+1)\gamma]_{K_3} \\ &= [(\sigma\tau-1)(\tau-1)\gamma]_{K_3} \\ &= [T_{K/K_3}((\tau-1)\gamma)]_{K_3}\end{aligned}$$

so $T((\tau-1)[\gamma]) \neq (0,0,0)$ and hence $(\tau-1)[\gamma] \neq 0$. Therefore $(\tau-1)[\gamma] = 0$ implies $T((\sigma-1)[\gamma]) = (0,0,0)$. □

Lemma 3.12. *If $[\gamma] \in J$, then there exists $\chi \in X$ such that $T((\tau-1)[\gamma+\chi]) = (0,0,0)$.*

Proof. We have $[T_{K/K_1}((\tau-1)\gamma)]_{K_1} = [0]_{K_1}$ because $(\tau-1)[\gamma] \in [K_1]$, so there are 4 cases:

case 1: $T((\tau-1)[\gamma]) = (0,0,0)$

Let $\chi = 0$.

case 2: $T((\tau-1)[\gamma]) = (0,a,a)$

Let $\chi = a\theta_a\theta_b$. Then $T((\tau-1)[\gamma+\chi]) = (0,a,a)+(0,a,a) = (0,0,0)$.

case 3: $T((\tau-1)[\gamma]) = (0,0,a)$

Let $\chi = c\theta_b + b\theta_a\theta_b$. Then $T((\tau-1)[\gamma+\chi]]) = (0,0,a)+(0,0,a) = (0,0,0)$.

case 4: $T((\tau-1)[\gamma]) = (0,a,0)$

Let $\chi = a\theta_a\theta_b + c\theta_b + b\theta_a\theta_b$. Then
$T((\tau-1)[\gamma+\chi]) = (0,a,a)+(0,0,a)+(0,a,0) = (0,0,0)$.

□

Proof of Theorem 3.9. By Corollary 3.8 we have $X^G = \langle [a\theta_a],[a\theta_b],[b\theta_b]\rangle_{\mathbb{F}_2}$, so each class in X^G has a nontrivial image under T. By Corollary 3.4 we have $Y^G = [F]$, so each class in Y^G has a trivial image. Thus $X^G \cap Y^G = \{[0]\}$, so $X \cap Y = \{[0]\}$ by Lemma 2.5.

Now let $[\gamma] \in J$ be arbitrary. Then there exists $[\chi] \in X$ such that $T((\tau-1)[\gamma+\chi]) = (0,0,0)$ by Lemma 3.12. Thus by Theorem 3.2 there exists $f \in F$ such that $(\tau-1)[\gamma+\chi] = [f]$ and by construction of Y there exists $k_f \in Y$ such that $T_{K/F}(k_f) = f$. This gives

$$(\tau-1)[\gamma+\chi+(\sigma-1)k_f] = (\tau-1)[\gamma+\chi] + T_{K/F}[k_f] = [f]+[f] = [0]$$

so by Lemma 3.11 we have

$$T((\sigma-1)[\gamma+\chi+(\sigma-1)k_f])=(0,0,0).$$

Thus by Theorem 3.2 there exists $f'\in F$ and $k_{f'}\in Y$ such that

$$T_{K/F}([k_{f'}])=[f']=(\sigma-1)[\gamma+\chi+(\sigma-1)k_f]$$

which gives

$$(\tau-1)[\gamma+\chi+(\sigma-1)k_f+(\tau-1)k_{f'}]=[f]+[f]+[0]=[0]$$

and

$$(\sigma-1)[\gamma+\chi+(\sigma-1)k_f+(\tau-1)k_{f'}]=[f']+[0]+[f']=[0].$$

Hence $[\gamma+\chi+(\sigma-1)k_f+(\tau-1)k_{f'}]$ is in J^G, so it is in $X^G+Y^G\subset X+Y$ by Lemma 3.10. Since $[\chi+(\sigma-1)k_f+(\tau-1)k_{f'}]\in X+Y$ and $(\sigma-1)k_f,(\tau-1)k_{f'}\in Y$, we have $[\gamma]\in X+Y$.

Therefore $J=X\oplus Y$. □

When Y is separated into its components $\langle[k_y]\rangle$, this is a decomposition of $X\oplus Y$ into indecomposable submodules.

Chapter 4

Decomposition for p odd

This chapter will present the general case, with emphasis on where it differs from Chapter 3. In particular, the construction of X requires significant additional work.

4.1 Notation

Let K/F be a Galois field extension of characteristic $p > 2$ with

$$\mathrm{Gal}(K/F) \cong \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z} = \langle \sigma, \tau \rangle .$$

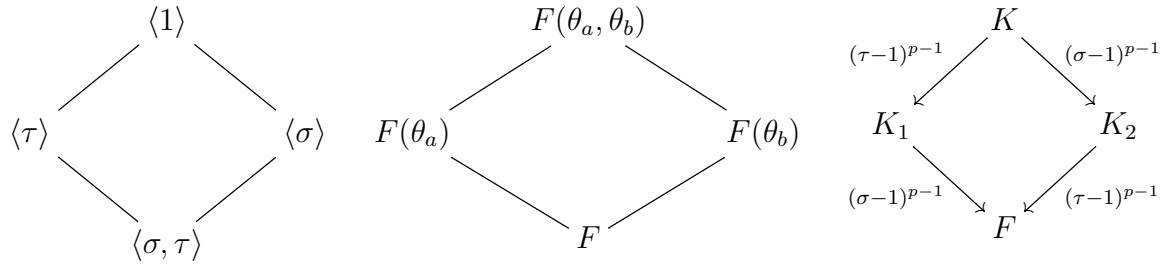
Again, we have

$$\begin{aligned} K_1 &= F(\theta_a) = \mathrm{Fix}\,\langle \tau \rangle \\ K_2 &= F(\theta_b) = \mathrm{Fix}\,\langle \sigma \rangle \\ J &= K^+/\wp(K) \end{aligned}$$

where θ_a and θ_b are roots of polynomials $x^p - x - a$ and $x^p - x - b$, respectively, and

$$\begin{aligned} \wp(K) &= \{k^p - k : k \in K\} \\ [f] &= f + \wp(K). \end{aligned}$$

Choose σ and τ so that $\sigma(\theta_a) = \theta_a + 1$ and $\tau(\theta_b) = \theta_b + 1$. Some subgroups, fixed fields, and trace maps are illustrated below:



(The intermediate field K_3 is omitted because there are now $p+1$ distinct proper intermediate fields.) Note that $(\tau - 1)^{p-1} = 1 + \tau + \cdots + \tau^{p-1}$ and $(\sigma - 1)^{p-1} = 1 + \sigma + \cdots + \sigma^{p-1}$ in characteristic p. Again, the compositions $T_{K/F} = T_{K_1/F} \circ T_{K/K_1} = T_{K_2/F} \circ T_{K/K_2}$ hold.

4.2 Supertrace

For $p = 2$, our decomposition relied on classifying elements by their images under the map T, which we affectionately call the supertrace. In order to generalize this approach, we need a process by which to identify classes in J representable by elements in $[F]$, preferably one whose complexity does not increase with the number of intermediate fields.

If L/K is a Galois field extension, then by the Fundamental Theorem of Galois Theory

$$\mathrm{Gal}(K/F) \cong \mathrm{Gal}(L/F)/\mathrm{Gal}(L/K)$$

which can be represented by the short exact sequence

$$1 \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(L/F) \to \mathrm{Gal}(K/F) \to 1$$

where the map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(L/F)$ is inclusion and map $\mathrm{Gal}(L/F) \to \mathrm{Gal}(K/F)$ takes an automorphism $\sigma\colon L \to L$ to its restriction $\sigma\colon K \to K$ (an automorphism by normality). For $[\gamma] \in J^G$, take

$$L = K(\theta_\gamma) = F(\theta_a, \theta_b, \theta_\gamma)$$

and denote lifts of generators σ and τ in $\mathrm{Gal}(K/F)$ by $\tilde{\sigma}$ and $\tilde{\tau}$ in $\mathrm{Gal}(L/F)$, respectively. This notation will be used throughout the section.

We will propose a sequence of conditions on γ in terms of trace maps that will limit the possibilities for $\mathrm{Gal}(L/F)$ in the short exact sequence and allow us to conclude that $[\gamma] \in [F]$.

Lemma 4.1. *If $k_2 \in K_2$ with $[k_2] = [0]$, then there exists $\ell \in \mathbb{F}_p$ such that $[k_2]_{K_2} = [\ell a]_{K_2}$.*

Proof. Same as for Lemma 3.1. □

Theorem 4.2. *If $[T_{K/K_1}(\gamma)]_{K_1} = [0]_{K_1}$, then there exists $k_1 \in K_1$ such that $[\gamma] = [k_1]$. Similarly, if $[T_{K/K_2}(\gamma)]_{K_2} = [0]_{K_2}$, then there exists $k_2 \in K_2$ such that $[\gamma] = [k_2]$.*

Proof. In Proposition 6.2 of [2]. □

Lemma 4.3. *We have $\tilde{\tau}^p = 1$ if and only if $[T_{K/K_1}(\gamma)]_{K_1} = [0]_{K_1}$ and $\tilde{\sigma}^p = 1$ if and only if $[T_{K/K_2}(\gamma)]_{K_2} = [0]_{K_2}$.*

Proof. Since $[\gamma] \in J^G$, we have $[T_{K/K_1}(\gamma)] = [0]$. Thus $[T_{K/K_1}(\gamma)]_{K_1} = [\ell b]_{K_1}$ for some $\ell \in \mathbb{F}_p$ by Lemma 4.1, so

$$(1 + \tilde{\tau} + \cdots + \tilde{\tau}^{p-1})\gamma = T_{K/K_1}(\gamma) = \ell b + k_1^p - k_1$$

for some $k_1 \in K_1$. Note that

$$\begin{aligned}(\ell\theta_b + k_1)^p - (\ell\theta_b + k_1) &= \ell(\theta_b^p - \theta_b) + k_1^p - k_1 \\ &= \ell b + k_1^p - k_1 \\ &= (1 + \tilde{\tau} + \cdots + \tilde{\tau}^{p-1})\gamma\end{aligned}$$

and

$$\begin{aligned}((1+\tilde{\tau}+\cdots+\tilde{\tau}^{p-1})\theta_\gamma)^p-(1+\tilde{\tau}+\cdots+\tilde{\tau}^{p-1})\theta_\gamma &= (1+\tilde{\tau}+\cdots+\tilde{\tau}^{p-1})(\theta_\gamma^p-\theta_\gamma)\\ &= (1+\tilde{\tau}+\cdots+\tilde{\tau}^{p-1})\gamma\end{aligned}$$

ie. $\ell\theta_b+k_1$ and $(1+\tilde{\tau}+\cdots+\tilde{\tau}^{p-1})\theta_\gamma$ are roots of the same Artin-Schreier polynomial, so

$$(1+\tilde{\tau}+\cdots+\tilde{\tau}^{p-1})\theta_\gamma=\ell\theta_b+k_1+z$$

for some $z\in\mathbb{F}_p$. Therefore

$$\begin{aligned}(\tilde{\tau}^p-1)\theta_\gamma &= (\tilde{\tau}-1)(1+\tilde{\tau}+\cdots+\tilde{\tau}^{p-1})\theta_\gamma\\ &= (\tilde{\tau}-1)(\ell\theta_b+k_1+z)\\ &= \tilde{\tau}(\ell\theta_b)+\tilde{\tau}(k_1)+\tilde{\tau}(z)-\ell\theta_b-k_1-z\\ &= \ell\tau(\theta_b)+k_1+z-\ell\theta_b-k_1-z\\ &= \ell(\theta_b+1)-\ell\theta_b\\ &= \ell.\end{aligned}$$

We also have

$$(\tilde{\tau}^p-1)\theta_a=\tau^p(\theta_a)-\theta_a=\theta_a-\theta_a=0$$

and

$$(\tilde{\tau}^p-1)\theta_b=\tau^p(\theta_b)-\theta_b=\theta_b+p-\theta_b=0$$

so $\tilde{\tau}^p-1=0$ if and only $\ell=0$. Therefore $\tilde{\tau}^p=1$ if and only if $[T_{K/K_1}(\gamma)]_{K_1}=[0]_{K_1}$. The proof for $\tilde{\sigma}$ is analagous. □

Lemma 4.4. *Suppose there exists $\gamma_2\in K_2$ such that $[\gamma_2]=[\gamma]$. Then $(\tau-1)[\gamma_2]_{K_2}=[0]_{K_2}$ if and only if $[\tilde{\sigma},\tilde{\tau}]=1$.*

Proof. It is sufficient to consider $L=K(\theta_{\gamma_2})$ because $K(\theta_\gamma)\cong K(\theta_{\gamma_2})$. Since $[\gamma_2]=[\gamma]\in J^G$ we have $(\tau-1)[\gamma_2]=[0]$, so $(\tau-1)[\gamma_2]_{K_2}=[\ell a]_{K_2}$ for some $\ell\in\mathbb{F}_p$ by Lemma 4.1. Choose $k_2\in K_2$ such that

$$\tau(\gamma_2)=\gamma_2+\ell a+k_2^p-k_2.$$

Note that

$$(\tilde{\sigma}(\theta_{\gamma_2}))^p-\tilde{\sigma}(\theta_{\gamma_2})=\tilde{\sigma}(\theta_{\gamma_2}^p-\theta_{\gamma_2})=\tilde{\sigma}(\gamma_2)=\sigma(\gamma_2)=\gamma_2$$

because $\gamma_2\in K_2$, so

$$\tilde{\sigma}(\theta_{\gamma_2})=\theta_{\gamma_2}+z_1$$

for some $z_1\in\mathbb{F}_p$. Applying $\tilde{\sigma}^{-1}$ to this equation gives

$$\tilde{\sigma}^{-1}(\theta_{\gamma_2})=\theta_{\gamma_2}-z_1.$$

We also have

$$(\tilde{\tau}(\theta_{\gamma_2}))^p-\tilde{\tau}(\theta_{\gamma_2})=\tilde{\tau}(\theta_{\gamma_2}^p-\theta_{\gamma_2})=\tilde{\tau}(\gamma_2)=\tau(\gamma_2)$$

and

$$\begin{aligned}(\theta_{\gamma_2} + \ell\theta_a + k_2)^p - (\theta_{\gamma_2} + \ell\theta_a + k_2) \\ &= \theta_{\gamma_2}^p - \theta_{\gamma_2} + \ell(\theta_a^p - \theta_a) + k_2^p - k_2 \\ &= \gamma_2 + k_2^p - k_2 = \tau(\gamma_2)\end{aligned}$$

ie. $\tilde{\tau}(\theta_{\gamma_2})$ and $\theta_{\gamma_2} + \ell\theta_a + k_2$ are roots of the same Artin-Schreier polynomial, so

$$\tilde{\tau}(\theta_{\gamma_2}) = \theta_{\gamma_2} + \ell\theta_a + k_2 + z_2$$

for some $z_2 \in \mathbb{F}_p$. Applying $\tilde{\tau}^{-1}$ to this equation gives

$$\tilde{\tau}^{-1}(\theta_{\gamma_2}) = \theta_{\gamma_2} - \ell\theta_a - \tilde{\tau}^{-1}(k_2) - z_2.$$

Therefore

$$\begin{aligned}[\tilde{\sigma}, \tilde{\tau}]\theta_{\gamma_2} &= \tilde{\sigma}\tilde{\tau}\tilde{\sigma}^{-1}\tilde{\tau}^{-1}(\theta_{\gamma_2}) \\ &= \tilde{\sigma}\tilde{\tau}\tilde{\sigma}^{-1}(\theta_{\gamma_2} - \ell\theta_a - \tilde{\tau}^{-1}(k_2) - z_2) \\ &= \tilde{\sigma}\tilde{\tau}(\theta_{\gamma_2} - z_1 - \ell(\theta_a - 1) - \tilde{\tau}^{-1}(k_2) - z_2) \\ &= \tilde{\sigma}(\theta_{\gamma_2} + \ell\theta_a + k_2 + z_2 - z_1 - \ell(\theta_a - 1) - \tilde{\tau}(\tilde{\tau}^{-1}(k_2)) - z_2) \\ &= \tilde{\sigma}(\theta_{\gamma_2} + \ell - z_1) \\ &= \theta_{\gamma_2} + \ell + z_1 - z_1 \\ &= \theta_{\gamma_2} + \ell.\end{aligned}$$

Since θ_a and θ_b are fixed by $\tilde{\tau}$ and $\tilde{\sigma}$, respectively,

$$[\tilde{\sigma}, \tilde{\tau}]\theta_a = \theta_a$$

and

$$[\tilde{\sigma}, \tilde{\tau}]\theta_b = \theta_b.$$

Thus $[\tilde{\sigma}, \tilde{\tau}] = 1$ if and only if $[\tilde{\sigma}, \tilde{\tau}]\theta_{\gamma_2} = \theta_{\gamma_2}$, which occurs precisely when $\ell = 0$, so $[\tilde{\sigma}, \tilde{\tau}] = 1$ if and only if $[(\tau - 1)\gamma_2]_{K_2} = [0]_{K_2}$. □

Note that if the second of the trace conditions in Lemma 4.3 is satisfied then Theorem 4.2 says that we can indeed find $\gamma_2 \in K_2$ such that $[\gamma_2] = [\gamma]$ and Lemma 4.1 says that $(\tau - 1)[\gamma_2]_{K_2} = [\ell a]_{K_2}$ for some $\ell \in \mathbb{F}_p$.

Analagously, if $[T_{K/K_1}(\gamma)]_{K_1} = [0]_{K_1}$, then there exists $\gamma_1 \in K_1$ such that $[\gamma_1] = [\gamma]$ and we have $[\tilde{\sigma}, \tilde{\tau}] = 1$ if and only if $[(\sigma - 1)\gamma_1]_{K_1} = [0]_{K_1}$. This gives the following corollary:

Corollary 4.5. *Let $\gamma \in J^G$. If there exist $\gamma_1 \in K_1$ and $\gamma_2 \in K_2$ such that $[\gamma] = [\gamma_1] = [\gamma_2]$, then $(\sigma - 1)[\gamma_1]_{K_1} = [0]_{K_1}$ if and only if $(\tau - 1)[\gamma_2]_{K_2} = [0]_{K_2}$.*

Theorem 4.6. *Suppose $\gamma \in J^G$ with $[T_{K/K_2}(\gamma)]_{K_2} = [0]_{K_2}$ and suppose $\gamma_2, \gamma_2' \in K_2$ such that $[\gamma] = [\gamma_2] = [\gamma_2']$. Then $(\tau - 1)[\gamma_2]_{K_2} = (\tau - 1)[\gamma_2']_{K_2}$.*

Proof. Let γ_2, γ_2' be as given. Then $[\gamma_2 - \gamma_2'] = [0]$ so $[\gamma_2 - \gamma_2']_{K_2} = [\ell a]_{K_2}$ for some $\ell \in \mathbb{F}_p$ by Lemma 4.1. Thus

$$(\tau - 1)[\gamma_2]_{K_2} = (\tau - 1)[\gamma_2' + \ell a]_{K_2} = (\tau - 1)[\gamma_2']_{K_2}$$

because ℓa is fixed by τ. □

Theorem 4.7. *Let $[\gamma] \in J^G$. Then $[\gamma] \in [F]$ if and only if the following conditions hold:*

- $[T_{K/K_1}(\gamma)]_{K_1} = [0]_{K_1}$
- $[T_{K/K_2}(\gamma)]_{K_2} = [0]_{K_2}$
- *There exists either $\gamma_1 \in K_1$ such that $[\gamma] = [\gamma_1]$ and $(\sigma - 1)[\gamma_1]_{K_1} = [0]_{K_1}$ or $\gamma_2 \in K_2$ such that $[\gamma] = [\gamma_2]$ and $(\tau - 1)[\gamma_2]_{K_2} = [0]_{K_2}$.*

Proof. Suppose $[\gamma] \in J^G$ satisfies these conditions and let $L = K(\theta_\gamma)$. We will show that $\mathrm{Gal}(L/F) \cong \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$. Since $|\mathrm{Gal}(L/F)| = p^3$, it is isomorphic to exactly 1 of the following:

$$\mathbb{Z}/p^3\mathbb{Z} \qquad \mathbb{Z}/p^2\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z} \qquad \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z} \qquad M_{p^3} \qquad H_{p^3}$$

(The last 2 are defined below.) By Lemmas 4.3 and 4.4 (and using the same notation), we have $\tilde{\sigma}^2 = \tilde{\tau}^2 = [\tilde{\sigma}, \tilde{\tau}] = 1$. Let μ generate $\mathrm{Gal}(L/K)$, which has order p, and let $\tilde{\mu}$ be its image, which also has order p.

- If $\mathrm{Gal}(L/F) \cong \mathbb{Z}/p^3\mathbb{Z}$, then

  $$\frac{\mathrm{Gal}(L/F)}{\mathrm{Gal}(L/K)} \cong \frac{\mathbb{Z}/p^3\mathbb{Z}}{\mathbb{Z}/p\mathbb{Z}} \cong \mathbb{Z}/p^2\mathbb{Z}$$

  which does not give $\mathrm{Gal}(K/F)$.

- If $\mathrm{Gal}(L/F) \cong \mathbb{Z}/p^2\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$, then $\mathrm{Gal}(L/K)$ is either $p\mathbb{Z}/p^2\mathbb{Z} \oplus 0$ or $\langle(\ell p, 1)\rangle$ for some $\ell \in \mathbb{F}_p$, which give the following quotients:

  $$\frac{\mathbb{Z}/p^2\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}}{p\mathbb{Z}/p^2\mathbb{Z} \oplus 0} \cong \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$$
  $$\frac{\mathbb{Z}/p^2\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}}{\langle(\ell p, 1)\rangle} \cong \mathbb{Z}/p^2\mathbb{Z}$$

  Only the former agrees with $\mathrm{Gal}(K/F)$, so we can take $\tilde{\mu} = (p, 0)$. At least 1 of σ and τ must have nonzero first coordinate in $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$. Without loss of generality assume that $\sigma = (m, n)$ where $m \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$, ie. $m \not\equiv 0 \pmod{p}$. Then $\tilde{\sigma} = (m + \ell p, n)$ for some $\ell \in \mathbb{Z}$. However this gives $|\tilde{\sigma}| = p^2$, a contradiction.

- Suppose $\mathrm{Gal}(L/F) \cong M_{p^3}$, the semidirect product $\mathbb{Z}/p\mathbb{Z} \ltimes \mathbb{Z}/p^2\mathbb{Z}$ with homomorphism $\phi\colon \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/p^2\mathbb{Z})$ given by $\phi(x)(y) = (xp + 1)y$, so that

  $$(x, y)(z, w) = (x + z, (zp + 1)y + w).$$

We will compute the commutator subgroup of this semidirect product. First note that the inverse of (x, y) is $(-x, (xp-1)y)$. Thus

$$[(x,y),(z,w)] = (x,y)(z,w)(-x,(xp-1)y)(-z,(zp-1)w) = (0,(yz-xw)p).$$

Elements of this form generate the subgroup $\langle(0,p)\rangle$ in $\mathbb{Z}/p\mathbb{Z} \ltimes \mathbb{Z}/p^2\mathbb{Z}$. Since $\mathrm{Gal}(K/F)$ is Abelian we must have $\langle(0,p)\rangle \subseteq \langle\tilde{\mu}\rangle$, and since they are the same size they must be equal. This gives

$$\frac{\mathbb{Z}/p\mathbb{Z} \ltimes \mathbb{Z}/p^2\mathbb{Z}}{\langle\tilde{\mu}\rangle} \cong \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$$

as desired. Like in the last case, a generator of $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$ must have nonzero second coordinate, say m. Then preimages have second coordinates $m + \ell p$ where $m \not\equiv 0 \mod p$, contradicting the orders of $\tilde{\sigma}$ and $\tilde{\tau}$.

- Finally, suppose $\mathrm{Gal}(L/F) \cong H_{p^3}$. Again, we will compute the commutator subgroup. Recall that

$$H_{p^3} = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{Z}/p\mathbb{Z} \right\}$$

is a group of 3-by-3 matrices under multiplication. We have

$$\begin{aligned} &\left[\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} \right] \\ &\quad = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -d & df-e \\ 0 & 1 & -f \\ 0 & 0 & 1 \end{pmatrix} \\ &\quad = \begin{pmatrix} 1 & 0 & af-cd \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \end{aligned}$$

which generates a subgroup of size p and a quotient isomorphic to

$$\left\{ \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, c \in \mathbb{Z}/p\mathbb{Z} \right\} \cong \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$$

with generators

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

By the computation above we have

$$\left[\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \right] = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

which contradicts the fact that $[\tilde{\sigma}, \tilde{\tau}] = 1$ for all lifts of generators σ and τ.

Therefore $\mathrm{Gal}(L/F) \cong \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$, so by the same argument as in the proof of Theorem 3.2 we have $[\gamma] \in [F]$. Conversely, if $[\gamma] \in [F]$, then there exists $\gamma' \in F$ such that $[\gamma] = [\gamma']$, so

- $[T_{K/K_1}(\gamma)]_{K_1} = [T_{K/K_1}(\gamma')]_{K_1} = [0]_{K_1}$
- $[T_{K/K_2}(\gamma)]_{K_2} = [T_{K/K_2}(\gamma')]_{K_2} = [0]_{K_2}$
- $(\sigma - 1)[\gamma']_{K_1} = [0]_{K_1}$ for $\gamma' \in K_1$

because γ' is fixed by σ and τ. □

Corollary 4.5 and Theorem 4.6 show that the two parts of the third condition in Theorem 4.7 are equivalent, and that the result of the computation does not depend on the choice of representative.

4.3 Construction of Y

The submodule Y is entirely analagous to that in the Klein 4-group case.

Definition 6. Let $\mathcal{I}$ be a basis for $[F]$ as an $\mathbb{F}_p$ vector space, and for each $[y] \in \mathcal{I}$ choose $k_y \in K$ such that $T_{K/F}(k_y) = y$. (Such a k_y exists by Corollary 2.4.) Define Y to be the $\mathbb{F}_p[\mathrm{Gal}(K/F)]$-span of the classes of these elements in J:

$$Y = \sum_{[y] \in \mathcal{I}} \langle [k_y] \rangle$$

Theorem 4.8. *If $[y_1], [y_2] \in \mathcal{I}$ and $[y_1] \neq [y_2]$, then $\langle [k_{y_1}] \rangle \cap \langle [k_{y_2}] \rangle = \{[0]\}$.*

Proof. We will show that $\langle [k_{y_1}] \rangle^G = \langle [y_1] \rangle_{\mathbb{F}_p}$. Since $[y_1] \in [F] \cap \langle [k_{y_1}] \rangle$ we have $\langle [y_1] \rangle_{\mathbb{F}_2} \subseteq \langle [k_{y_1}] \rangle^G$. Let $[y] \in \langle [k_{y_1}] \rangle^G$. By Lemma 2.7

$$[y] = \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} \alpha_{ij} (\sigma - 1)^i (\tau - 1)^j [k_{y_1}]$$

for some $\alpha_{ij} \in \mathbb{F}_p$. Suppose for contradiction that there exist i, j not both $p-1$ such that $\alpha_{ij} \neq 0$. Let m be the maximum index such that $\alpha_{mj} \neq 0$ for some j and let n be the maximum index such that $\alpha_{mn} \neq 0$. Then at least one of $p - m - 1$ and $p - n - 1$ is greater than 0, so

$$[0] = (\sigma - 1)^{p-m-1} (\tau - 1)^{p-n-1} [y] = \sum_{i=0}^{m} \sum_{j=0}^{n} \alpha_{ij} (\sigma - 1)^{p+i-m-1} (\tau - 1)^{p+j-n-1} [k_{y_1}]$$

by hypothesis, and by choice of m and n, the only nonzero coefficient is α_{mn}. This gives

$$[0] = \alpha_{mn} (\sigma - 1)^{p-1} (\tau - 1)^{p-1} [k_{y_1}] = \alpha_{mn} T_{K/F} [k_{y_1}] = \alpha_{mn} [y_1] \neq [0]$$

which is a contradiction, so $\alpha_{ij} = 0$ unless $i = j = p-1$. Therefore

$$[y] = \alpha_{p-1,p-1}(\sigma - 1)^{p-1}(\tau - 1)^{p-1}[k_{y_1}] = \alpha_{p-1,p-1}[y_1]$$

so $\langle [k_{y_1}] \rangle^G = \langle [y_1] \rangle_{\mathbb{F}_p}$.

Since $[y_1]$ and $[y_2]$ are linearly independent over $\mathbb{F}_p$, we have $\langle [y_1] \rangle_{\mathbb{F}_p} \cap \langle [y_2] \rangle_{\mathbb{F}_p} = \{[0]\}$. Hence $\langle [k_{y_1}] \rangle \cap \langle [k_{y_2}] \rangle = \{[0]\}$ by Lemma 2.5. □

Therefore

$$Y = \bigoplus_{[y] \in \mathcal{J}} \langle [k_y] \rangle .$$

This module will be fixed for the remainder of Chapter 4.

Corollary 4.9. $Y^G = [F]$.

4.4 Construction of X

Instead of seeking an explicit fixed element $[x]$ as in Section 3.4, we will abstractly construct generators with properties that mirror those of $[a\theta_a]$ and $[c\theta_b + b\theta_a\theta_b]$. The main theorem is stated now and proven later in this section.

Theorem 4.10. *There exist $\alpha_R, \alpha_L \in K$ such that the following conditions hold, where $T_{K/K_1}(\alpha_L) = \beta_L$ and $= T_{K/K_2}(\alpha_R) = \beta_R$:*

- $[\beta_L], [\beta_R] \in J^G$
- $[T_{K/K_2}(\beta_L)]_{K_2} = [\ell a]_{K_2}$ *for some nonzero* $\ell \in \mathbb{F}_p$ *and* $[T_{K/K_1}(\beta_R)]_{K_1} = [b]_{K_1}$
- $(\sigma - 1)[\beta_L]_{K_1} = [0]_{K_1}$ *and* $(\tau - 1)[\beta_R]_{K_2} = [0]_{K_2}$
- $(\sigma - 1)[\alpha_L] = (\tau - 1)[\alpha_R]$

First, we assert the existence of elements β_L and β_R with the desired supertrace. This will use a classical theorem about solvable extension problems.

Theorem 4.11 (Witt)**.** *Let be K/F is a Galois field extension of characteristic p and G a group. If there exists a short exact sequence*

$$0 \to \mathbb{Z}/p\mathbb{Z} \to G \to \mathrm{Gal}(K/F) \to 0$$

that is central and nonsplit, then there exists a Galois field extension L/K that solves the corresponding embedding problem (described in Section 4.2).

Proof. From [4] via Appendix A of [5]. □

Theorem 4.12. *Let $\ell \in \mathbb{F}_p$. Then there exists $\beta_L \in K_1$ such that $[\beta_L] \in J^G$ and*

- $[T_{K/K_2}(\beta_L)]_{K_2} = [\ell a]_{K_2}$

- $(\sigma - 1)[\beta_L]_{K_1} = [0]_{K_1}$.

Similarly, there exists $\beta_R \in K_2$ such that $[\beta_R] \in J^G$ and

- $[T_{K/K_1}(\beta_R)]_{K_1} = [\ell b]_{K_1}$
- $(\tau - 1)[\beta_R]_{K_2} = [0]_{K_2}$.

Proof. Consider the following short exact sequence

$$0 \to \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p^2\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z} \to 0$$

with maps given by $n \mapsto (np, 0)$ and $(n_1, n_2) \mapsto (n_1 \mod p, n_2)$. Since $\mathbb{Z}/p^2\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$ is Abelian, the extension is nonsplit, and $\mathrm{Gal}(K/F) \cong \mathbb{Z}/p \oplus \mathbb{Z}/p$, there exists a Galois extension L/K with $\mathrm{Gal}(L/K) \cong \mathbb{Z}/p\mathbb{Z}$ and $\mathrm{Gal}(L/F) \cong \mathbb{Z}/p^2\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$ by Theorem 4.11.

According to Theorem 1.2, there exists $\gamma \in K$ such that $L = K(\theta_\gamma)$, and since L/K is Galois $[\gamma] \in J^G$. Note that lifts $\tilde{\sigma}$ and $\tilde{\tau}$ of generators σ and τ have orders p^2 and p in $\mathrm{Gal}(L/F)$. Take $|\tilde{\sigma}| = p^2$ and $|\tilde{\tau}| = p$. Then by Lemma 4.3 we have $[T_{K/K_2}(\gamma)]_{K_2} \neq [0]_{K_2}$ and $[T_{K/K_1}(\gamma)]_{K_1} = [0]_{K_1}$. Since $[\gamma] \in J^G$ there exists some nonzero $\tilde{\ell} \in \mathbb{F}_p$ such that $[T_{K/K_2}(\gamma)]_{K_2} = [\tilde{\ell} a]_{K_2}$ by Lemma 4.1. Then $[\gamma] \in [K_1]$ by Theorem 4.2, so we can choose $\beta \in K_1$ such that $[\ell\tilde{\ell}^{-1}\gamma] = [\beta]$. This gives

$$[T_{K/K_1}(\beta)]_{K_1} = \ell\tilde{\ell}^{-1}[T_{K/K_1}(\gamma)]_{K_1} = \ell\tilde{\ell}^{-1}[\tilde{\ell} a]_{K_1} = [\ell a]_{K_1}$$

Finally, note that $[\tilde{\sigma}, \tilde{\tau}] = 1$ because $\mathbb{Z}/p^2 \oplus \mathbb{Z}/p\mathbb{Z}$ is Abelian. Thus by Lemma 4.4 we have $(\sigma - 1)[\beta]_{K_1} = \ell\tilde{\ell}^{-1}[0]_{K_1} = [0]_{K_1}$. □

Now we identify a particular fixed class, which will eventually play the role of $[x]$.

Theorem 4.13. *If $[T_{K/K_2}(\beta_L)]_{K_2} = [\ell a]_{K_2}$ for some nonzero $\ell \in \mathbb{F}_p$ and $T_{K/K_1}(\alpha_L) = \beta_L$ then $(\sigma - 1)^{p-1}(\tau - 1)^{p-2}[\alpha_L] \in J^G$ with the following:*

- $[T_{K/K_1}((\sigma - 1)^{p-1}(\tau - 1)^{p-2}\alpha_L)]_{K_1} = [0]_{K_1}$
- $[T_{K/K_2}((\sigma - 1)^{p-1}(\tau - 1)^{p-2}\alpha_L)]_{K_2} = [0]_{K_2}$
- $(\tau - 1)[(\sigma - 1)^{p-1}(\tau - 1)^{p-2}\alpha_L]_{K_2} = [\ell a]_{K_2}$

Similarly, if $[T_{K/K_1}(\beta_R)]_{K_1} = [\ell b]_{K_1}$ and $T_{K/K_2}(\alpha_R) = \beta_R$, then $(\sigma - 1)^{p-2}(\tau - 1)^{p-1}[\alpha_R] \in J^G$ with the following:

- $[T_{K/K_1}((\sigma - 1)^{p-2}(\tau - 1)^{p-1}\alpha_R)]_{K_1} = [0]_{K_1}$
- $[T_{K/K_2}((\sigma - 1)^{p-2}(\tau - 1)^{p-1}\alpha_R)]_{K_2} = [0]_{K_2}$
- $(\sigma - 1)[(\sigma - 1)^{p-2}(\tau - 1)^{p-1}\alpha_R]_{K_1} = [\ell b]_{K_1}$

Proof. We have $(\sigma-1)^{p-1}(\tau-1)^{p-2}[\alpha_L] \in J^G$ because

$$(\sigma-1)^{p-1}(\tau-1)^{p-2}\alpha_L = (\tau-1)^{p-2}T_{K/K_2}(\alpha_L) \in K_2 = \operatorname{Fix}\langle\sigma\rangle$$

and

$$\begin{aligned}(\tau-1)[(\sigma-1)^{p-1}(\tau-1)^{p-2}\alpha_L] &= T_{K/F}[\alpha_L] \\ &= [T_{K/K_2}(T_{K/K_1}(\alpha_L))] \\ &= [T_{K/K_2}(\beta_L)] \\ &= [\ell a] \\ &= [0]\end{aligned}$$

(where $[T_{K/K_2}(\beta_L)]_{K_2} = [\ell a]_{K_2}$ implies $[T_{K/K_2}(\beta_L)] = [\ell a]$). Since $(\sigma-1)^{p-1}(\tau-1)^{p-2}[\alpha_L]$ is in the image of $\sigma-1$ and $\tau-1$, we also have

$$[T_{K/K_1}((\sigma-1)^{p-1}(\tau-1)^{p-2}\alpha_L)]_{K_1} = [0]_{K_1}$$

and

$$[T_{K/K_2}((\sigma-1)^{p-1}(\tau-1)^{p-2}\alpha_L)]_{K_2} = [0]_{K_2}$$

because $(\sigma-1)^p = (\tau-1)^p = 0$. Finally

$$\begin{aligned}[(\tau-1)(\sigma-1)^{p-1}(\tau-1)^{p-2}\alpha_L]_{K_2} &= [T_{K/F}(\alpha_L)]_{K_2} \\ &= [T_{K/K_2}(T_{K/K_1}(\alpha_L))]_{K_2} \\ &= [T_{K/K_2}(\beta_L)]_{K_2} \\ &= [\ell a]_{K_2}.\end{aligned}$$

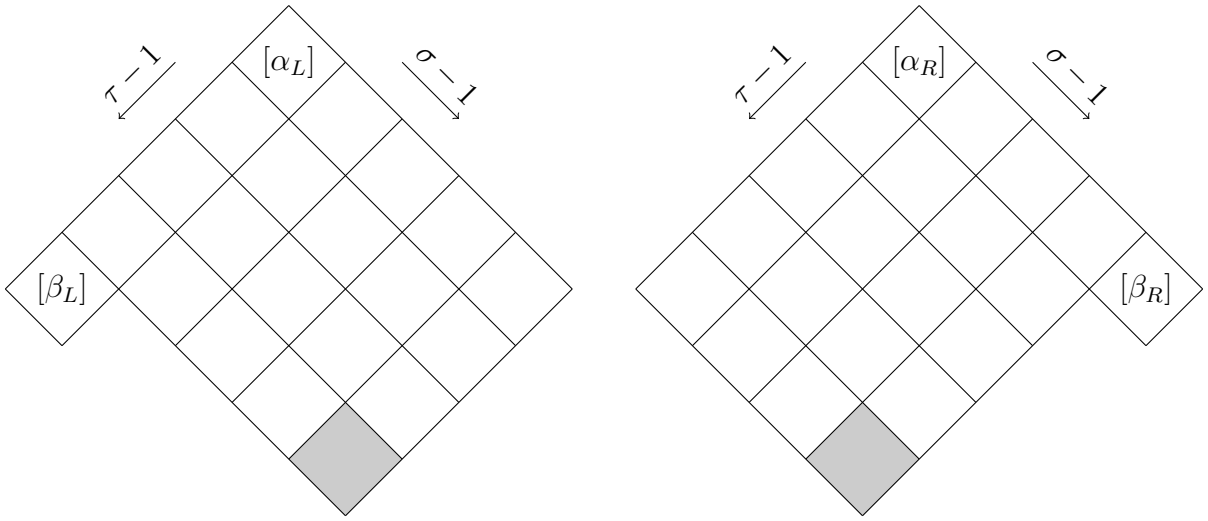
□

For the following 3 lemmas, let $\ell \in \mathbb{F}_p$ be nonzero and assume that $\alpha_L, \alpha_R, \beta_L, \beta_R \in K$ are such that:

- $T_{K/K_1}(\alpha_L) = \beta_L$ and $T_{K/K_2}(\alpha_R) = \beta_R$
- $[\beta_L], [\beta_R] \in J^G$
- $[T_{K/K_2}(\beta_L)]_{K_2} = [\ell a]_{K_2}$ for some nonzero $\ell \in \mathbb{F}_p$ and $[T_{K/K_1}(\beta_R)]_{K_1} = [b]_{K_1}$
- $(\sigma-1)[\beta_L]_{K_1} = [0]_{K_1}$ and $(\tau-1)[\beta_R]_{K_2} = [0]_{K_2}$

These exist by Theorem 4.12 and Corollary 2.4 and satisfy the hypotheses of Theorem 4.13. We will progressively adjust $[\alpha_L]$ and $[\alpha_R]$ by a sequence of elements $[\chi]$ with the goal of obtaining the relation $(\sigma-1)[\alpha_L] = (\tau-1)[\alpha_R]$.

Using Theorem 4.13, the submodules generated by $[\alpha_L]$ and $[\alpha_R]$ can be visualized as elements in boxes of a grid, where steps down and left denote application of $\tau-1$ and steps down and right application of $\sigma-1$, shown here for $p=5$.



We start by "gluing" the bottom most elements, shaded above.

Lemma 4.14. *There exists $\chi \in K$ such that*

$$(\sigma-1)^{p-1}(\tau-1)^{p-2}[\alpha_L+\chi] = (\sigma-1)^{p-2}(\tau-1)^{p-1}[\alpha_R]$$

and $T_{K/K_1}(\alpha_L+\chi) = \ell'\ell^{-1}\beta_L$ for some nonzero $\ell' \in \mathbb{F}_p$.

Proof. Choose $k_2 \in K_2$ such that $[(\sigma-1)^{p-2}(\tau-1)^{p-1}\alpha_R] = [k_2]$, which is possible by Theorem 4.2. Then $(\tau-1)[k_2]_{K_2} \neq [0]_{K_2}$ by Theorem 4.13 and Corollary 4.5, so by Lemma 4.1 there exists nonzero $\ell' \in \mathbb{F}_p$ such that $(\tau-1)[k_2]_{K_2} = [\ell' a]_{K_2}$.

This gives $(\sigma-1)^{p-2}(\tau-1)^{p-2}[(\tau-1)\alpha_R - (\sigma-1)(\ell'\ell^{-1}\alpha_L)] \in J^G$ with

$$[T_{K/K_1}((\sigma-1)^{p-2}(\tau-1)^{p-2}((\tau-1)\alpha_R - (\sigma-1)(\ell'\ell^{-1}\alpha_L)))]_{K_1} = [0-\ell'\ell^{-1}0]_{K_1} = [0]_{K_1}$$
$$[T_{K/K_2}((\sigma-1)^{p-2}(\tau-1)^{p-2}((\tau-1)\alpha_R - (\sigma-1)(\ell'\ell^{-1}\alpha_L)))]_{K_2} = [0-\ell'\ell^{-1}0]_{K_2} = [0]_{K_2}$$

and $[k_2 - (\sigma-1)^{p-1}(\tau-1)^{p-2}(\ell'\ell^{-1}\alpha_L)] = (\sigma-1)^{p-2}(\tau-1)^{p-2}[(\tau-1)\alpha_R - (\sigma-1)(\ell'\ell^{-1}\alpha_L)]$ with

$$(\tau-1)[k_2 - (\sigma-1)^{p-1}(\tau-1)^{p-2}(\ell'\ell^{-1}\alpha_L)]_{K_2} = [\ell' a - \ell' a]_{K_2} = [0]_{K_2}.$$

Therefore by Theorem 4.7 and the construction of Y there exists $\rho \in K$ such that

$$T_{K/F}[\rho] = [k_2 - (\sigma-1)^{p-1}(\tau-1)^{p-2}(\ell'\ell^{-1}\alpha_L)].$$

Let $\chi = (\tau-1)\rho + (\ell'\ell^{-1}-1)\alpha_L$. Then

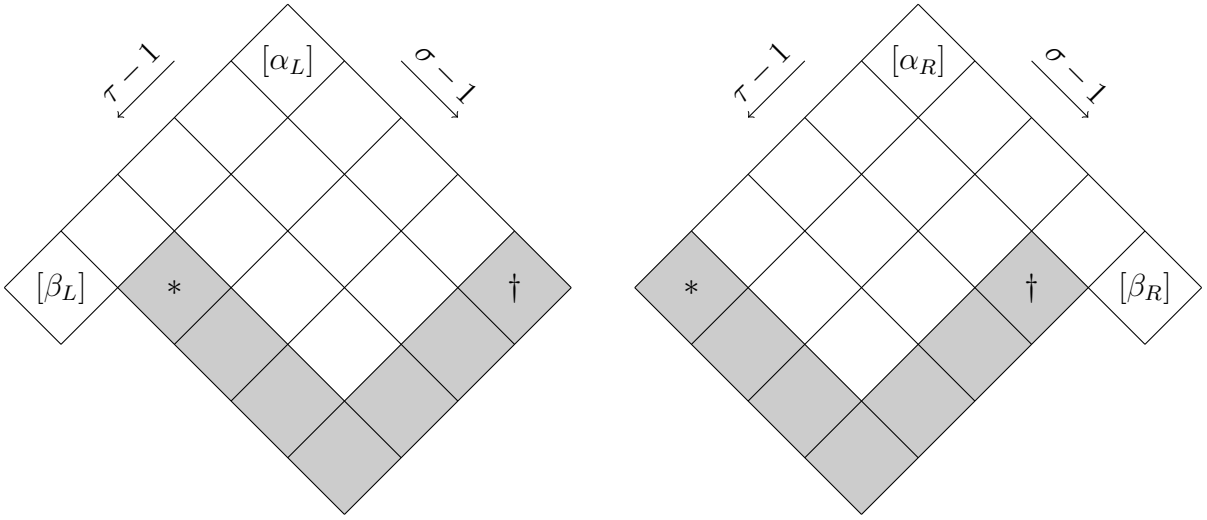
$$\begin{aligned}
&(\sigma-1)^{p-1}(\tau-1)^{p-2}[\alpha_L+\chi] \\
&\qquad = (\sigma-1)^{p-1}(\tau-1)^{p-2}[\ell'\ell^{-1}\alpha_L + (\tau-1)\rho] \\
&\qquad = (\sigma-1)^{p-1}(\tau-1)^{p-2}[\ell'\ell^{-1}\alpha_L] + T_{K/F}[\rho] \\
&\qquad = (\sigma-1)^{p-1}(\tau-1)^{p-2}[\ell'\ell^{-1}\alpha_L] + [k_2 - (\sigma-1)^{p-1}(\tau-1)^{p-2}(\ell'\ell^{-1}\alpha_L)] \\
&\qquad = [k_2] \\
&\qquad = (\sigma-1)^{p-2}(\tau-1)^{p-1}[\alpha_R]
\end{aligned}$$

and

$$T_{K/K_1}(\alpha_L + \chi) = T_{K/K_1}(\ell'\ell^{-1}\alpha_L + (\tau - 1)\rho) = \ell'\ell^{-1}\beta_L$$

because the second term is in the image of $\tau - 1$. □

Now we prove an inductive step to move us up and left, or, by switching σ and τ, up and right, gluing the bottom sides as illustrated below. (Matching symbols will align.)



Lemma 4.15. *If*

$$(\sigma - 1)^{i+1}(\tau - 1)^{p-2}[\alpha_L] = (\sigma - 1)^i(\tau - 1)^{p-1}[\alpha_R]$$

for some $1 \leq i \leq p - 2$ *then there exists* $\chi \in K$ *such that*

$$(\sigma - 1)^i(\tau - 1)^{p-2}[\alpha_L + \chi] = (\sigma - 1)^{i-1}(\tau - 1)^{p-1}[\alpha_R]$$

and $T_{K/K_1}[\alpha_L + \chi] = [\beta_L]$.

Proof. We have

$$(\sigma - 1)(\sigma - 1)^{i-1}(\tau - 1)^{p-2}[(\tau - 1)\alpha_R - (\sigma - 1)\alpha_L] = [0]$$

by hypothesis and

$$\begin{aligned}(\tau - 1)(\sigma - 1)^{i-1}(\tau - 1)^{p-2}&[(\tau - 1)\alpha_R - (\sigma - 1)\alpha_L] \\ &= (\sigma - 1)^{i-1}[(\tau - 1)^p\alpha_R - (\sigma - 1)T_{K/K_1}(\alpha_L)] \\ &= (\sigma - 1)^{i-1}[0 - (\sigma - 1)\beta_L] \\ &= [0]\end{aligned}$$

because $\beta_L \in J^G$, so

$$(\sigma - 1)^{i-1}(\tau - 1)^{p-2}[(\tau - 1)\alpha_R - (\sigma - 1)\alpha_L] \in J^G.$$

We also have

$$[T_{K/K_1}((\sigma-1)^{i-1}(\tau-1)^{p-2}((\tau-1)\alpha_R-(\sigma-1)\alpha_L))]_{K_1}=[0]_{K_1}$$

and

$$[T_{K/K_2}((\sigma-1)^{i-1}(\tau-1)^{p-2}((\tau-1)\alpha_R-(\sigma-1)\alpha_L))]_{K_2}=[0]_{K_2}$$

because both terms are in the image of $\tau-1$ and $\sigma-1$ for $2\leq i\leq p-2$ and when $i=1$

$$[T_{K/K_2}((\tau-1)^{p-1}\alpha_R)]_{K_2}=[T_{K/K_1}(\beta_R)]_{K_2}=[b]_{K_2}=[0]_{K_2}.$$

Choose $k_2\in K_2$ such that

$$(\sigma-1)^{i-1}(\tau-1)^{p-2}[(\tau-1)\alpha_R-(\sigma-1)\alpha_L]=[k_2]$$

which is possible by Theorem 4.2. Then $[(\tau-1)k_2]_{K_2}=[\ell' a]_{K_2}$ for some $\ell'\in\mathbb{F}_p$ by Lemma 4.1. By Theorem 4.13 this gives

$$(\tau-1)[k_2-(\sigma-1)^{p-1}(\tau-1)^{p-2}(\ell'\ell^{-1}\alpha_L)]_{K_2}=[\ell' a-\ell' a]_{K_2}=[0]_{K_2}.$$

Adjustment by $[(\sigma-1)^{p-1}(\tau-1)^{p-2}(\ell'\ell^{-1}\alpha_L)]$ does not affect the first 2 conditions of the supertrace because this class is in the image of $\sigma-1$ and $\tau-1$. Thus by Theorem 4.7 and the construction of Y there exists some $\rho\in K$ such that

$$T_{K/F}[\rho]=[k_2-(\sigma-1)^{p-1}(\tau-1)^{p-2}(\ell'\ell^{-1}\alpha_L)].$$

Let $\chi=(\sigma-1)^{p-i-1}(\tau-1)\rho+(\sigma-1)^{p-i-1}(\ell'\ell^{-1}\alpha_L)$. Then

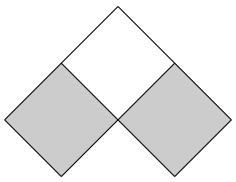
$$\begin{aligned}
&(\sigma-1)^i(\tau-1)^{p-2}[\alpha_L+\chi]\\
&\quad=(\sigma-1)^i(\tau-1)^{p-2}[\alpha_L+(\sigma-1)^{p-i-1}(\tau-1)\rho+(\sigma-1)^{p-i-1}(\ell'\ell^{-1}\alpha_L)]\\
&\quad=(\sigma-1)^i(\tau-1)^{p-2}[\alpha_L]+T_{K/F}[\rho]+(\sigma-1)^{p-1}(\tau-1)^{p-2}[\ell'\ell^{-1}\alpha_L]\\
&\quad=(\sigma-1)^i(\tau-1)^{p-2}[\alpha_L]+[k_2-(\sigma-1)^{p-1}(\tau-1)^{p-2}(\ell'\ell^{-1}\alpha_L)]+(\sigma-1)^{p-1}(\tau-1)^{p-2}[\ell'\ell^{-1}\alpha_L]\\
&\quad=(\sigma-1)^{i-1}(\tau-1)^{p-2}[(\sigma-1)\alpha_L]+[k_2]\\
&\quad=(\sigma-1)^{i-1}(\tau-1)^{p-2}[(\tau-1)\alpha_R]\\
&\quad=(\sigma-1)^{i-1}(\tau-1)^{p-1}[\alpha_R]
\end{aligned}$$

and

$$\begin{aligned}
T_{K/K_1}[\alpha_L+\chi]&=T_{K/K_1}[\alpha_L+(\sigma-1)^{p-i-1}(\tau-1)\rho+(\sigma-1)^{p-i-1}(\ell'\ell^{-1}\alpha_L)]\\
&=[\beta_L]+[0]+(\sigma-1)^{p-i-1}[\ell'\ell^{-1}\beta_L]\\
&=[\beta_L]
\end{aligned}$$

because the second term is in the image of $\tau-1$ and $\beta_L\in J^G$. □

Finally, we prove a similar lemma that glues units of the following shape, where the shaded elements are already attached.



This allows us to move through the remainder of the diagram and prove the theorem.

Lemma 4.16. *If*

$$(\sigma-1)^{i+1}(\tau-1)^{j-1}[\alpha_L] = (\sigma-1)^i(\tau-1)^j[\alpha_R]$$

and

$$(\sigma-1)^{i}(\tau-1)^{j}[\alpha_L] = (\sigma-1)^{i-1}(\tau-1)^{j+1}[\alpha_R]$$

for some $1 \leq i, j \leq p-2$ *then there exists some* $\chi \in K$ *such that*

$$(\sigma-1)^{i}(\tau-1)^{j-1}[\alpha_L+\chi] = (\sigma-1)^{i-1}(\tau-1)^{j}[\alpha_R]$$

and $T_{K/K_1}[\alpha_L+\chi] = [\beta_L]$.

Proof. We have

$$(\sigma-1)(\sigma-1)^{i-1}(\tau-1)^{j-1}[(\tau-1)\alpha_R-(\sigma-1)\alpha_L] = [0]$$

and

$$(\tau-1)(\sigma-1)^{i-1}(\tau-1)^{j-1}[(\tau-1)\alpha_R-(\sigma-1)\alpha_L] = [0]$$

by hypothesis, so

$$(\sigma-1)^{i-1}(\tau-1)^{j-1}[(\tau-1)\alpha_R-(\sigma-1)\alpha_L] \in J^G.$$

We also have

$$[T_{K/K_1}((\sigma-1)^{i-1}(\tau-1)^{j-1}((\tau-1)\alpha_R-(\sigma-1)\alpha_L))]_{K_1} = [0]_{K_1}$$

because both terms are in the image of $\tau-1$ for $2 \leq j \leq p-2$ and when $j=1$

$$[T_{K/K_1}((\sigma-1)^{i}\alpha_L)]_{K_1} = (\sigma-1)^{i-1}[(\sigma-1)\beta_L]_{K_1} = (\sigma-1)^{i-1}[0]_{K_1} = [0]_{K_1}.$$

Similarly

$$[T_{K/K_2}((\sigma-1)^{i-1}(\tau-1)^{j-1}((\tau-1)\alpha_R-(\sigma-1)\alpha_L))]_{K_2} = [0]_{K_2}$$

because both terms are in the image of $\sigma-1$ for $2 \leq i \leq p-2$ and when $i=1$

$$[T_{K/K_2}((\tau-1)^{j}\alpha_R)]_{K_2} = (\tau-1)^{j-1}[(\tau-1)\alpha_R]_{K_2} = (\tau-1)^{j-1}[0]_{K_2} = [0]_{K_2}.$$

Choose $k_2 \in K_2$ such that

$$(\sigma-1)^{i-1}(\tau-1)^{j-1}[(\tau-1)\alpha_R-(\sigma-1)\alpha_L] = [k_2]$$

which is possible by Theorem 4.2. Then $[(\tau-1)k_2]_{K_2} = [\ell' a]_{K_2}$ for some $\ell' \in \mathbb{F}_p$ by Lemma 4.1. By Theorem 4.13 this gives

$$(\tau-1)[k_2-(\sigma-1)^{p-1}(\tau-1)^{p-2}(\ell'\ell^{-1}\alpha_L)]_{K_2} = [\ell' a-\ell' a]_{K_2} = [0]_{K_2}.$$

Adjustment by $[(\sigma-1)^{p-1}(\tau-1)^{p-2}(\ell'\ell^{-1}\alpha_L)]$ does not affect the first 2 conditions of the supertrace because this class is in the image of $\sigma-1$ and $\tau-1$. Thus by Theorem 4.7 and the construction of Y there exists some $\rho \in K$ such that

$$T_{K/F}[\rho] = [k_2-(\sigma-1)^{p-1}(\tau-1)^{p-2}(\ell'\ell^{-1}\alpha_L)].$$

Let $\chi = (\sigma-1)^{p-i-1}(\tau-1)^{p-j}\rho + (\sigma-1)^{p-i-1}(\tau-1)^{p-j-1}(\ell'\ell^{-1}\alpha_L)$. Then

$$\begin{aligned}
&(\sigma-1)^i(\tau-1)^{j-1}[\alpha_L+\chi] \\
&\quad= (\sigma-1)^i(\tau-1)^{j-1}[\alpha_L + (\sigma-1)^{p-i-1}(\tau-1)^{p-j}\rho + (\sigma-1)^{p-i-1}(\tau-1)^{p-j-1}(\ell'\ell^{-1}\alpha_L)] \\
&\quad= (\sigma-1)^i(\tau-1)^{j-1}[\alpha_L] + T_{K/F}[\rho] + (\sigma-1)^{p-1}(\tau-1)^{p-2}[\ell'\ell^{-1}\alpha_L] \\
&\quad= (\sigma-1)^i(\tau-1)^{j-1}[\alpha_L] + [k_2 - (\sigma-1)^{p-1}(\tau-1)^{p-2}(\ell'\ell^{-1}\alpha_L)] + (\sigma-1)^{p-1}(\tau-1)^{p-2}[\ell'\ell^{-1}\alpha_L] \\
&\quad= (\sigma-1)^{i-1}(\tau-1)^{j-1}[(\sigma-1)\alpha_L] + [k_2] \\
&\quad= (\sigma-1)^{i-1}(\tau-1)^{j-1}[(\tau-1)\alpha_R] \\
&\quad= (\sigma-1)^{i-1}(\tau-1)^{j}[\alpha_R]
\end{aligned}$$

and

$$\begin{aligned}
T_{K/K_1}[\alpha_L+\chi] &= T_{K/K_1}[\alpha_L + (\sigma-1)^{p-i-1}(\tau-1)\rho + (\sigma-1)^{p-i-1}(\ell'\ell^{-1}\alpha_L)] \\
&= [\beta_L] + [0] + (\sigma-1)^{p-i-1}[\ell'\ell^{-1}\beta_L] \\
&= [\beta_L]
\end{aligned}$$

because the second term is in the image of $\tau-1$ and $\beta_L \in J^G$. □

Proof of Theorem 4.10. Such choices of β_L, β_R exist by Theorem 4.12 and preimages α_L, α_R under T_{K/K_1} and T_{K/K_2}, respectively, can be taken by Corollary 2.4. This satisfies the conditions for Lemma 4.14, which adjusts α_L so that

$$(\sigma-1)^{p-1}(\tau-1)^{p-2}[\alpha_L] = (\sigma-1)^{p-2}(\tau-1)^{p-1}[\alpha_R]$$

and $T_{K/K_1}[\alpha_L] = [\ell'\ell^{-1}\beta_L]$ for some nonzero $\ell' \in \mathbb{F}_p$, which we can eliminate by multiplying α_L by $\ell(\ell')^{-1}$. Lemma 4.15 gives us

$$(\sigma-1)^i(\tau-1)^{p-2}[\alpha_L] = (\sigma-1)^{i-1}(\tau-1)^{p-1}[\alpha_R]$$

for all $1 \le i \le p-1$ and, by exchanging σ and τ,

$$(\sigma-1)^{p-1}(\tau-1)^{j-1}[\alpha_L] = (\sigma-1)^{p-2}(\tau-1)^{j}[\alpha_R]$$

for all $1 \le j \le p-1$, and finally

$$(\sigma-1)^i(\tau-1)^{j-1}[\alpha_L] = (\sigma-1)^{i-1}(\tau-1)^{j}[\alpha_R]$$

for all $1 \le i, j \le p-1$ after application of Lemma 4.16, which includes

$$(\sigma-1)[\alpha_L] = (\tau-1)[\alpha_R].$$

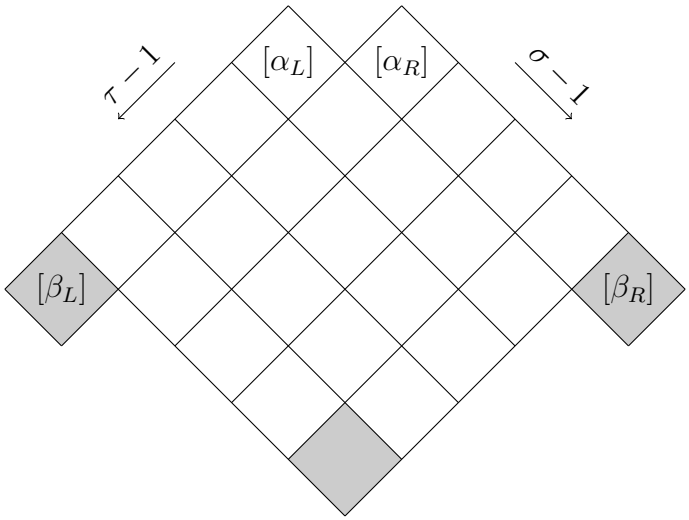
None of these steps alters the conditions on β_L or β_R. □

Definition 7. Let α_L and α_R be given as in Theorem 4.10 and define X to be the $\mathbb{F}_p[\mathrm{Gal}(K/F)]$-span of their classes in J:

$$X = \langle [\alpha_L], [\alpha_R] \rangle$$

This submodule will be fixed for the remainder of Chapter 4.

Here is a picture of X in the style used earlier, which may be a useful reference for proofs later in this chapter or in Section 2.2. Shaded elements are fixed.



As in Section 3.4, we will show that our X has the form described in Section 2.2.

Theorem 4.17. *If $\delta_1, \delta_2, \delta_3 \in \mathbb{F}_p$ with*

$$\delta_1(\tau-1)^{p-1}[\alpha_L] + \delta_2(\sigma-1)^{p-1}(\tau-1)^{p-2}[\alpha_L] + \delta_3(\sigma-1)^{p-1}[\alpha_R] = [f]$$

for some $f \in F$, then $\delta_1 = \delta_2 = \delta_3 = 0$.

Proof. Using the notation in Theorem 4.10, this can be rewritten as

$$\delta_1[\beta_L] + \delta_2(\sigma-1)^{p-1}(\tau-1)^{p-2}[\alpha_L] + \delta_3[\beta_R] = [f]$$

By choice of α_R and Theorem 4.13

$$\begin{aligned}[0]_{K_1} &= [T_{K/K_1}(f)]_{K_1} \\ &= [T_{K/K_1}(\delta_1\beta_L + \delta_2(\sigma-1)^{p-1}(\tau-1)^{p-2}\alpha_L + \delta_3\beta_R)]_{K_1} \\ &= [0]_{K_1} + [0]_{K_1} + [\delta_3 b]_{K_1}\end{aligned}$$

so $\delta_3 = 0$. Analagously $\delta_1 = 0$ because $\ell \neq 0$. Finally

$$\begin{aligned}[0]_{K_2} &= (\tau-1)[f]_{K_2} \\ &= (\tau-1)[\delta_2(\sigma-1)^{p-1}(\tau-1)^{p-2}\alpha_L]_{K_2} \\ &= [\delta_2 \ell a]_{K_2}\end{aligned}$$

by Theorems 4.13 and 4.6, so $\delta_2 = 0$. □

Corollary 4.18. *The submodule X is indecomposable.*

Proof. From Theorem 2.14. □

Corollary 4.19. $X^G = \langle (\tau-1)^{p-1}[\alpha_L], (\sigma-1)^{p-1}(\tau-1)^{p-2}[\alpha_L], (\sigma-1)^{p-1}[\alpha_R] \rangle_{\mathbb{F}_p}$.

Proof. From Corollary 2.12. □

4.5 Structure of J

Theorem 4.20. *If $X = \langle [\alpha_L], [\alpha_R] \rangle$ and $Y = \bigoplus_{[y] \in \mathcal{J}} \langle [k_y] \rangle$ as defined above, then*

$$J = X \oplus Y.$$

Lemma 4.21. *Let $[\gamma] \in J$. If $(\sigma - 1)^{i-1}(\tau - 1)^{p-1}[\gamma] = [0]$ for some $1 \leq i \leq p-1$ then $[T_{K/K_1}((\sigma - 1)^i \gamma)]_{K_1} = [0]_{K_1}$.*

Proof. Since $(\sigma - 1)^{i-1}(\tau - 1)^{p-1}\gamma \in K_1$ and $(\sigma - 1)^{i-1}(\tau - 1)^{p-1}[\gamma] = [0]$ we have

$$[(\sigma - 1)^{i-1}(\tau - 1)^{p-1}\gamma]_{K_1} = [lb]_{K_1}$$

for some $l \in \mathbb{F}_p$ by Lemma 4.1. Thus

$$\begin{aligned} [T_{K/K_1}((\sigma - 1)^i \gamma)]_{K_1} &= [(\sigma - 1)(\sigma - 1)^{i-1}(\tau - 1)^{p-1}\gamma]_{K_1} \\ &= [(\sigma - 1)lb]_{K_1} \\ &= [0]_{K_1} \end{aligned}$$

as desired. □

Proof of Theorem 4.20. Suppose $[\gamma] \in X^G \cap Y^G$. Then $[\gamma] \in [F]$ because $Y^G = [F]$ (Corollary 4.9) and

$$[\gamma] = \delta_1(\tau - 1)^{p-1}[\alpha_L] + \delta_2(\sigma - 1)^{p-1}(\tau - 1)^{p-2}[\alpha_L] + \delta_3[\beta_R]$$

for some $\delta_1, \delta_2, \delta_3 \in \mathbb{F}_p$ by Corollary 3.8. Then $\delta_1, \delta_2, \delta_3 = 0$ by Theorem 4.17 so $[\gamma] = [0]$. Thus $X \cap Y = \{[0]\}$ by Lemma 2.5 so $X + Y = X \oplus Y$. We will now show that $X \oplus Y = J$.

Let $[\gamma] \in J$ be arbitrary. We will induct on the following parameter:

$$s_{[\gamma]} = |\{(i,j) : (\sigma - 1)^i(\tau - 1)^j[\gamma] \neq [0]\}|$$

base case:

If $s_{[\gamma]} = 0$ then $[\gamma] = [0]$ so $[\gamma] \in J$.

Suppose $s_{[\gamma]} = 1$. Then $[\gamma] \in J^G$, so

$$[T_{K/K_1}(\gamma)]_{K_1} = [l_1 b]_{K_1}$$

and

$$[T_{K/K_2}(\gamma)]_{K_2} = [l_2 a]_{K_2}$$

for some $l_1, l_2 \in \mathbb{F}_p$ by Lemma 4.1. Then

$$\begin{aligned} &[T_{K/K_1}(\gamma - l_1(\sigma - 1)^{p-1}\alpha_R - l_2\ell^{-1}(\tau - 1)^{p-1}\alpha_L)]_{K_1} \\ &\qquad = [l_1 b]_{K_1} - [l_1 b]_{K_1} - [l_2\ell^{-1}0]_{K_1} \\ &\qquad = [0]_{K_1} \\ &[T_{K/K_2}(\gamma - l_1(\sigma - 1)^{p-1}\alpha_R - l_2\ell^{-1}(\tau - 1)^{p-1}\alpha_L)]_{K_2} \\ &\qquad = [l_2 a]_{K_2} - [l_1 0]_{K_2} - [l_2\ell^{-1}\ell a]_{K_2} \\ &\qquad = [0]_{K_2} \end{aligned}$$

by Theorem 4.10, so by Theorem 4.2 we can choose $k_2 \in K_2$ such that

$$[k_2] = [\gamma - l_1(\sigma-1)^{p-1}\alpha_R - l_2\ell^{-1}(\tau-1)^{p-1}\alpha_L]$$

and there exists $l_3 \in \mathbb{F}_p$ such that

$$(\tau-1)[k_2]_{K_2} = [l_3 a]_{K_2}.$$

Let $[\gamma'] = [\gamma - l_1(\sigma-1)^{p-1}\alpha_R - l_2\ell^{-1}(\tau-1)^{p-1}\alpha_L - l_3\ell^{-1}(\sigma-1)^{p-1}(\tau-1)^{p-2}\alpha_L]$.

Then $[\gamma'] \in J^G$ because all its terms are, and we still have $[T_{K/K_1}(\gamma')]_{K_1} = [0]_{K_1}$ and $[T_{K/K_2}(\gamma')]_{K_2} = [0]_{K_2}$ because the last term is in the image of $\sigma - 1$ and $\tau - 1$. However

$$(\tau-1)[k_2 - l_3\ell^{-1}(\sigma-1)^{p-1}(\tau-1)^{p-2}\alpha_L]_{K_2} = [l_3 a]_{K_2} - [l_3\ell^{-1}\ell a]_{K_2} = [0]_{K_2}$$

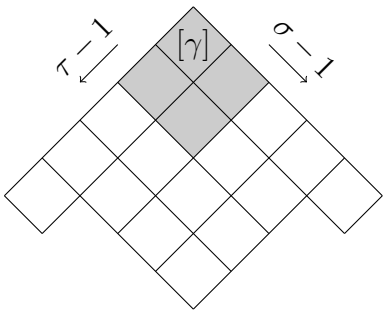
by Theorem 4.13 so $[\gamma'] \in [F]$ by Theorem 4.7 and thus $[\gamma'] \in Y$. Hence

$$[\gamma] = [\gamma'] + [l_1(\sigma-1)^{p-1}\alpha_R + l_2\ell^{-1}(\tau-1)^{p-1}\alpha_L + l_3\ell^{-1}(\sigma-1)^{p-1}(\tau-1)^{p-2}\alpha_L]$$

where the first term is in Y and the remainder in X, so $[\gamma] \in X \oplus Y$.

inductive step: Suppose $s_{[\gamma]} > 1$ and $[\gamma'] \in X \oplus Y$ for all $[\gamma'] \in J$ with $s_{[\gamma']} < s_{[\gamma]}$. We will illustrate cases by deleting elements that must be zero and shading those that must be nonzero. In each case we seek to eliminate at least one fixed element generated by $[\gamma]$.

case 1: $(\sigma-1)(\tau-1)[\gamma] \neq [0]$ and $(\sigma-1)^i(\tau-1)^{p-1}[\gamma] = (\sigma-1)^{p-1}(\tau-1)^j[\gamma] = [0]$ for all $1 \leq i, j \leq p-1$.



Let m be the maximum index such that $(\sigma-1)^m(\tau-1)[\gamma] \neq [0]$ and let n be the maximum index such that $(\sigma-1)^m(\tau-1)^n[\gamma] \neq [0]$. Then $(\sigma-1)^m(\tau-1)^n[\gamma] \in J^G$. Note that $1 \leq m, n \leq p-2$ in this case. Thus $(\sigma-1)^m(\tau-1)^n[\gamma]$ is in the image of both $\sigma - 1$ and $\tau - 1$, so

$$[T_{K/K_1}((\sigma-1)^m(\tau-1)^n\gamma)]_{K_1} = [0]_{K_1}$$

and

$$[T_{K/K_2}((\sigma-1)^m(\tau-1)^n\gamma)]_{K_2} = [0]_{K_2}.$$

Choose $k_2 \in K_2$ such that

$$(\sigma-1)^m(\tau-1)^n[\gamma] = [k_2]$$

which is possible by Theorem 4.2. Then by Lemma 4.1

$$(\tau-1)[k_2]_{K_2} = [la]_{K_2}$$

for some $l \in \mathbb{F}_p$. Consider $[\gamma - l\ell^{-1}(\sigma-1)^{p-m-1}(\tau-1)^{p-n-2}\alpha_L] \in J$. We still have

$$[T_{K/K_1}((\sigma-1)^m(\tau-1)^n(\gamma - l\ell^{-1}(\sigma-1)^{p-m-1}(\tau-1)^{p-n-2}))\alpha_L]_{K_1} = [0]_{K_1}$$

and

$$[T_{K/K_2}((\sigma-1)^m(\tau-1)^n(\gamma - l\ell^{-1}(\sigma-1)^{p-m-1}(\tau-1)^{p-n-2}))\alpha_L]_{K_2} = [0]_{K_2}$$

but

$$(\tau-1)[k_2 - l\ell^{-1}(\sigma-1)^{p-1}(\tau-1)^{p-2}\alpha_L]_{K_2} = [la - l\ell^{-1}\ell a] = [0]_{K_2}.$$

Thus by Theorem 4.7 $(\sigma-1)^m(\tau-1)^n[\gamma - l\ell^{-1}(\sigma-1)^{p-m-1}(\tau-1)^{p-n-2}\alpha_L] \in [F]$, so by construction of Y there exists $[k] \in Y$ such that

$$T_{K/F}[k] = (\sigma-1)^m(\tau-1)^n[\gamma - l\ell^{-1}(\sigma-1)^{p-m-1}(\tau-1)^{p-n-2}\alpha_L].$$

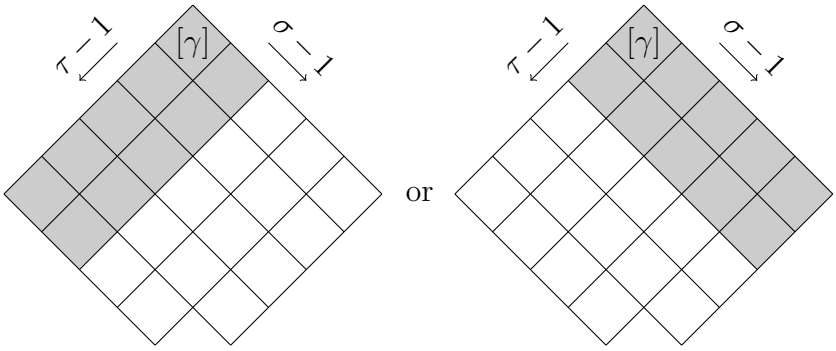
Let $[\gamma'] = [\gamma - l\ell^{-1}(\sigma-1)^{p-m-1}(\tau-1)^{p-n-2}\alpha_L - (\sigma-1)^{p-m-1}(\tau-1)^{p-n-1}k] \in J$.

Since $l\ell^{-1}(\sigma-1)^{p-m-1}(\tau-1)^{p-n-2}[\alpha_L] \in X$ and $(\sigma-1)^{p-m-1}(\tau-1)^{p-n-1}[k] \in Y$, we have $[\gamma'] \in X \oplus Y$ if and only if $[\gamma] \in X \oplus Y$. Moreover

$$\begin{aligned}
&(\sigma-1)^m(\tau-1)^n[\gamma'] \\
&\quad= (\sigma-1)^m(\tau-1)^n[\gamma] - l\ell^{-1}(\sigma-1)^{p-1}(\tau-1)^{p-2}[\alpha_L] - (\sigma-1)^{p-1}(\tau-1)^{p-1}[k] \\
&\quad= (\sigma-1)^m(\tau-1)^n[\gamma] - l\ell^{-1}(\sigma-1)^{p-1}(\tau-1)^{p-2}[\alpha_L] - T_{K/F}[k] \\
&\quad= (\sigma-1)^m(\tau-1)^n[\gamma] - l\ell^{-1}(\sigma-1)^{p-1}(\tau-1)^{p-2}[\alpha_L] \\
&\qquad- (\sigma-1)^m(\tau-1)^n[\gamma - l\ell^{-1}(\sigma-1)^{p-m-1}(\tau-1)^{p-n-2}\alpha_L] \\
&\quad= [0] \\
&(\sigma-1)^{m+1}[\gamma'] \\
&\quad= (\sigma-1)^{m+1}[\gamma] - l\ell^{-1}(\sigma-1)^{p}(\tau-1)^{p-n-2}[\alpha_L] - (\sigma-1)^{p}(\tau-1)^{p-n-1}[k] \\
&\quad= [0] \\
&(\tau-1)^{n+1}[\gamma'] \\
&\quad= (\tau-1)^{n+1}[\gamma] - l\ell^{-1}(\sigma-1)^{p-m-1}(\tau-1)^{p-1}[\alpha_L] - (\sigma-1)^{p-m-1}(\tau-1)^{p}[k] \\
&\quad= [0] - l\ell^{-1}(\sigma-1)^{p-m-2}(\tau-1)^{p}[\alpha_R] - [0] \\
&\quad= [0]
\end{aligned}$$

so the previously nonzero element in the (m,n)-th position has been eliminated without affecting any that were previously zero. Hence $s_{[\gamma']} < s_{[\gamma]}$.

case 2: $(\sigma-1)^i(\tau-1)^{p-1}[\gamma] \neq [0]$ or $(\sigma-1)^{p-1}(\tau-1)^j[\gamma] \neq [0]$ for some $1 \leq i, j \leq p-1$ and $(\sigma-1)^{p-1}(\tau-1)^{p-1}[\gamma] = [0]$



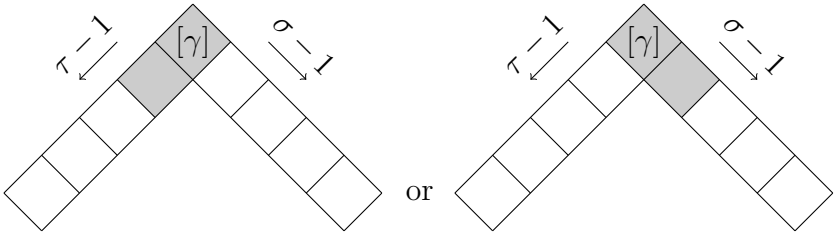
Construct $[\gamma']$ as in case 1, since the assumption that $m \leq p-2$ is used only in the final displayed equation, where $p-m-2$ appears in the exponent of $(\sigma-1)$. Thus $(\sigma-1)^m(\tau-1)^n[\gamma'] = (\sigma-1)^{m+1}[\gamma'] = [0]$ but $(\tau-1)^{n+1}[\gamma]$ may be nonzero, so it is not necessarily true that $s_{[\gamma']} < s_{[\gamma]}$. However

$$
\begin{aligned}
&(\tau-1)^{n+1}(\sigma-1)[\gamma'] \\
&\quad = (\tau-1)^{n+1}(\sigma-1)[\gamma] - l\ell^{-1}(\sigma-1)^{p-m}(\tau-1)^{p-1}[\alpha_L] - (\sigma-1)^{p-m}(\tau-1)^p[k] \\
&\quad = [0] - l\ell^{-1}(\sigma-1)^{p-m-1}(\tau-1)^p[\alpha_R] - [0] \\
&\quad = [0] \\
&(\tau-1)^{n+2}[\gamma'] \\
&\quad = (\tau-1)^{n+2}[\gamma] - l\ell^{-1}(\sigma-1)^{p-m-1}(\tau-1)^p[\alpha_L] - (\sigma-1)^{p-m-1}(\tau-1)^{p+1}[k] \\
&\quad = [0]
\end{aligned}
$$

so at worst we have eliminated 1 nonzero element and added 1 more. Thus $s_{[\gamma']} \leq s_{[\gamma]}$. If $s_{[\gamma]} \leq s_{[\gamma']}$ then we can apply the induction assumption, and if not we can replace $[\gamma]$ with $[\gamma']$ and repeat the inductive step.

Each time that case 2 occurs an element $(\sigma-1)^i(\tau-1)^j[\gamma]$ with either $i = p-1$ or $j = p-1$ will be eliminated and one with either $i = 0$ or $j = 0$ may be created. This can occur at most $2(p-2)$ times (corresponding to the elements that appear in the diagram for case 2 and not that for case 1), after which $[\gamma]$ will fall under another case and we can apply the induction assumption.

case 3: $(\sigma-1)(\tau-1)[\gamma] = [0]$



Let m be the maximum index such that $(\sigma-1)^m[\gamma] \neq [0]$ or $(\tau-1)^m[\gamma] \neq [0]$. Note that $m \geq 1$ because $s_{[\gamma]} \geq 2$, and without loss of generality assume the former is nonzero. Then

$$(\sigma-1)[(\sigma-1)^m\gamma] = [0]$$

by choice of m and

$$(\tau-1)[(\sigma-1)^m\gamma] = (\sigma-1)^{m-1}[(\sigma-1)(\tau-1)\gamma] = [0]$$

by assumption, so $(\sigma-1)^m[\gamma] \in J^G$. If $m \geq 2$ then

$$(\sigma-1)^{m-1}(\tau-1)^{p-1}[\gamma] = (\sigma-1)^{m-2}(\tau-1)^{p-2}[(\sigma-1)(\tau-1)\gamma] = [0]$$

by assumption, and if $m = 1$ then

$$(\sigma-1)^{m-1}(\tau-1)^{p-1}[\gamma] = (\tau-1)^{p-1}[\gamma] = [0]$$

by choice of m, so by Lemma 4.21

$$[T_{K/K_1}((\sigma-1)^m\gamma)]_{K_1} = [0]_{K_1}.$$

Since $(\sigma-1)^m[\gamma]$ is in the image of $\sigma-1$

$$[T_{K/K_2}((\sigma-1)^m\gamma)]_{K_2} = [0]_{K_2}$$

as well. Choose $k_2 \in K_2$ such that

$$(\sigma-1)^m[\gamma] = [k_2]$$

which is possible by Theorem 4.2. Then by Lemma 4.1

$$(\tau-1)[k_2]_{K_2} = [la]_{K_2}$$

for some $l \in \mathbb{F}_p$. Consider $[\gamma - l\ell^{-1}(\sigma-1)^{p-m-1}(\tau-1)^{p-2}\alpha_L] \in J$. We still have

$$[T_{K/K_1}((\sigma-1)^m(\gamma - l\ell^{-1}(\sigma-1)^{p-m-1}(\tau-1)^{p-2}))\alpha_L]_{K_1} = [0]_{K_1}$$

and

$$[T_{K/K_2}((\sigma-1)^m(\gamma - l\ell^{-1}(\sigma-1)^{p-m-1}(\tau-1)^{p-2}))\alpha_L]_{K_2} = [0]_{K_2}$$

but

$$(\tau-1)[k_2 - l\ell^{-1}(\sigma-1)^{p-1}(\tau-1)^{p-2}\alpha_L]_{K_2} = [la - l\ell^{-1}\ell a] = [0]_{K_2}.$$

Thus by Theorem 4.7 we have $(\sigma-1)^m[\gamma - l\ell^{-1}(\sigma-1)^{p-m-1}(\tau-1)^{p-2}\alpha_L] \in [F]$, so there exists $[k] \in Y$ such that

$$T_{K/F}[k] = (\sigma-1)^m[\gamma - l\ell^{-1}(\sigma-1)^{p-m-1}(\tau-1)^{p-2}\alpha_L].$$

Let $[\gamma'] = [\gamma - l\ell^{-1}(\sigma-1)^{p-m-1}(\tau-1)^{p-2}\alpha_L - (\sigma-1)^{p-m-1}(\tau-1)^{p-1}k] \in J$.

Since $l\ell^{-1}(\sigma-1)^{p-m-1}(\tau-1)^{p-2}[\alpha_L] \in X$ and $(\sigma-1)^{p-m-1}(\tau-1)^{p-1}[k] \in Y$, we have $[\gamma'] \in X \oplus Y$ if and only if $[\gamma] \in X \oplus Y$. Moreover

$$\begin{aligned}
&(\sigma-1)^m[\gamma'] \\
&\quad = (\sigma-1)^m[\gamma] - l\ell^{-1}(\sigma-1)^{p-1}(\tau-1)^{p-2}[\alpha_L] - (\sigma-1)^{p-1}(\tau-1)^{p-1}[k] \\
&\quad = (\sigma-1)^m[\gamma] - l\ell^{-1}(\sigma-1)^{p-1}(\tau-1)^{p-2}[\alpha_L] - T_{K/F}[k] \\
&\quad = (\sigma-1)^m[\gamma] - l\ell^{-1}(\sigma-1)^{p-1}(\tau-1)^{p-2}[\alpha_L] \\
&\qquad - (\sigma-1)^m[\gamma - l\ell^{-1}(\sigma-1)^{p-m-1}(\tau-1)^{p-2}\alpha_L] \\
&\quad = [0] \\
&(\sigma-1)^{m+1}[\gamma'] \\
&\quad = (\sigma-1)^{m+1}[\gamma] - l\ell^{-1}(\sigma-1)^{p}(\tau-1)^{p-2}[\alpha_L] - (\sigma-1)^{p}(\tau-1)^{p-1}[k] \\
&\quad = [0]
\end{aligned}$$

Let n be the maximum index such that $(\tau-1)^n[\gamma] \neq [0]$. Then

$$\begin{aligned}
&(\tau-1)^{n+1}[\gamma'] \\
&\quad = (\tau-1)^{n+1}[\gamma] - l\ell^{-1}(\sigma-1)^{p-m-1}(\tau-1)^{p+n-1}[\alpha_L] - (\sigma-1)^{p-m-1}(\tau-1)^{p+n}[k] \\
&\quad = [0] - l\ell^{-1}(\sigma-1)^{p-m-1}(\tau-1)^{p+n-1}[\alpha_L] - [0].
\end{aligned}$$

If $n \geq 1$ then this term is $[0]$ because $(\tau-1)^p = 0$. If $n = 0$ and $m \leq p-2$ then this term is $[0]$ because $(\tau-1)^{p-1}[\alpha_L] \in J^G$. If $n = 0$ and $m = p-1$ then $(\tau-1)[\gamma] = [0]$ and $[(\sigma-1)^{p-1}\gamma] = [k_2]$ with $(\sigma-1)^{p-1}\gamma, k_2 \in K_2$ so

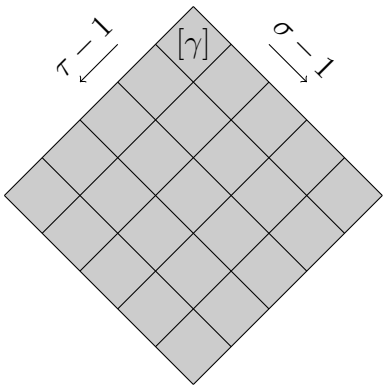
$$(\tau-1)[(\sigma-1)^{p-1}\gamma]_{K_2} = [T_{K/K_2}((\tau-1)\gamma)]_{K_2} = [T_{K/K_2}(0)]_{K_2} = [0]_{K_2}$$

by Corollary 2.2 and

$$(\tau-1)[(\sigma-1)^{p-1}\gamma]_{K_2} = (\tau-1)[k_2]_{K_2} = [la]_{K_2}$$

by Theorem 4.6, which gives $l = 0$. Thus $(\tau-1)^{n+1}[\gamma'] = [0]$, so the previously nonzero element in the (m,n)-th position has been eliminated without affecting any that were previously zero. Hence $s_{[\gamma']} < s_{[\gamma]}$.

case 4: $(\sigma-1)^{p-1}(\tau-1)^{p-1}[\gamma] \neq [0]$



Then $(\sigma-1)^{p-1}(\tau-1)^{p-1}[\gamma] = T_{K/F}[\gamma] \in [F]$, so there exists $[k] \in Y$ such that $T_{K/F}[k] = T_{K/F}[\gamma]$. Let $[\gamma'] = [\gamma - k]$. Then

$$(\sigma-1)^{p-1}(\tau-1)^{p-1}[\gamma'] = T_{K/F}[\gamma - k] = [0]$$

so $s_{[\gamma']} < s_{[\gamma]}$ and $[\gamma'] \in X \oplus Y$ if and only if $[\gamma] \in X \oplus Y$.

In each case there exists $[\gamma'] \in J$ such that $s_{[\gamma']} < s_{[\gamma]}$ and $[\gamma] \in X \oplus Y$ if and only if $[\gamma'] \in X \oplus Y$, so $[\gamma'] \in X \oplus Y$ by the induction hypothesis and thus $[\gamma] \in X \oplus Y$.

Therefore $[\gamma] \in X \oplus Y$ for all $[\gamma] \in J$. □

Bibliography

[1] Frank A. Chemotti, *Galois Module Structure for Square Classes of Units in Klein 4-Group Extensions*, Undergraduate Thesis, Davidson College, May 13, 2005.

[2] Andrew Schultz, *Parameterizing solutions to any Galois embedding problem over $\mathbb{Z}/p^n\mathbb{Z}$ with elementary p-Abelian kernel*, Journal of Algebra **411** (2014), 50-91.

[3] J. Mináč, A. Schultz, and J. Swallow, *Galois module structure of pth-power classes of cyclic extensions of degree p^n*, Proceedings of the London Mathematical Society **92** (2006), 307-341.

[4] E. Witt, *Konstruktion von galoisschen Körpern der Charakeristik p zu vorgegebener Gruppe der Ordnung p^f*, J. Reine Angew. Math. **174** (1936), 237-245.

[5] Christian U. Jensen, Arne Ledet, and Noriko Yui, *Generic Polynomials: Constructive Aspects of the Inverse Galois Problem*, Mathematical Sciences Research Institute Publications, vol. 45, 2002.